MINISTRY OF URBAN DEVELOPMENT, CONSTRUCTION AND HOUSING

SRI LANKA LAND DEVELOPMENT CORPORATION

Purchase of Computer and Server Virus Protection Software for SLLDC Head Office

Procurement No: **S/105/25**

Closing Date :- 22nd April 2025

Closing times :- 13.30 hours

Section I. Instructions to Vendors (ITV)

A: General	
1. Scope of Bid	1.1 The Purchaser named in the Data Sheet invites you to submit a quotation for the supply of Goods as specified in Section III Schedule of Requirements. Upon receipt of this invitation, you are requested to acknowledge the receipt of this invitation and your intention to submit a quotation. The Purchaser may not consider you for inviting quotations in the future, if you failed to acknowledge the receipt of this invitation or not submitting a quotation after expressing the intention as above.
B: Contents of Documents	
2. Contents of Documents	2.1 The documents consist of the Sections indicated below. • Section I. Instructions to Vendors(ITV) • Section II. Data Sheet • Section III. Schedule of Requirements • Section IV. Technical Specifications &Mandatory Requirement that shall be fulfilled by the vender • Section V. Quotation submission Form(s) 2.2 Purchase of Bidding Document
C: Preparation of Quotation	
3. Documents Comprising your Quotation	3.1 The Quotation shall comprise the following: (a) Quotation Submission Form and the Price Schedules; (b) Technical Specifications & Compliance with Specifications

4. Quotation Submission Form and Price Schedules	4.1 The vendor shall submit the Quotation Submission Form using the form furnished in Section V. This form must be completed without any alterations to its format, and no substitutes shall be accepted. All blank spaces shall be filled in with the information requested. 4.2 Alternative offers shall not be considered. The vendors are advised not to quote different options for the same item but furnish the most competitive another options available to the bidder.
5. Prices and Discounts	5.1 Unless specifically stated in Data Sheet, all items must be priced separately in the Price Schedules. 5.2 The price to be quoted in the Quotation Submission Form shall be the total price of the Quotation, including any discounts offered. 5.3 The applicable VAT shall be indicated separately. 5.4 Prices quoted by the vendor shall be fixed during the vendor's performance of the Contract and not subject to variation on any account. A Quotation submitted with an adjustable price shall be treated as non-responsive and may be rejected.
6. Currency	6.1 The vendors shall quote only in Sri Lanka Rupees.
7. Documents to Establish the Conformity of the Goods	7.1 The vendor shall furnish as part of its quotation the documentary evidence that the Goods conform to the technical specifications and standards specified in Section IV, "Technical Specifications & Compliance with Specifications". 7.2 The documentary evidence may be in the form of literature, drawings or data, and shall consist of a detailed item by item description of the essential technical and performance characteristics of the Goods, demonstrating substantial responsiveness of the Goods to the technical specifications, and if applicable, a statement of deviations and exceptions to the provisions of the Technical Specifications given. 7.3 If stated in the Data Sheet the vendor shall submit a certificate from the manufacturer to demonstrate that it has been duly authorized by the

	manufacturer or producer of the Goods to supply these Goods in Sri Lanka.
8. Period of Validity of quotation	8.1 Quotations shall remain valid for the period of sixty (60) days after the quotation submission deadline date.
9. Format and Signing of Quotation	9.1 The quotation shall be typed or written in indelible ink and shall be signed by a person duly authorized to sign on behalf of the vendor.
D: Submission and Opening of Quotation	
10. Submission of Quotation	10.1 Vendors may submit their quotations by mail or by hand in sealed envelopes addressed to the Purchaser bear the specific identification of the contract number. 10.2 If the quotation is not sealed and marked as required, the Purchaser will assume no responsibility for the misplacement or premature opening of the quotation.
11. Deadline for Submission of Quotation	11.1 Quotation must be received by the Purchaser at the address set out in Section II, "Data Sheet", and no later than the date and time as specified in the Data Sheet.
12. Late Quotations	12.1 The Purchaser shall reject any quotation that arrives after the deadline for submission of quotations, in accordance with ITV Clause 11.1 above.
13. Opening of Quotations	13.1 The Purchaser shall conduct the opening of quotation in publican the address, date and time specified in the Data Sheet. 13.2 A representative of the bidders may be present and mark its attendance.
E: Evaluation and Comparison of Quotation	
14. Clarifications	14.1 To assist in the examination, evaluation and comparison of the quotations, the Purchaser may, at its discretion, ask any vendor for a

	clarification of its quotation. Any clarification submitted by a vendor in respect to its quotation which is not in response to a request by the Purchaser shall not be considered. 14.2 The Purchaser's request for clarification and the response shall be in writing.
15. Responsiveness of Quotations	15.1 The Purchaser will determine the responsiveness of the quotation to the documents based on the contents of the quotation received. 15.2 If a quotation is evaluated as not substantially responsive to the documents issued, it may be rejected by the Purchaser.
16. Evaluation of quotation	16.1 The Purchaser shall evaluate each quotation that has-been determined, to be substantially responsive. 16.2 To evaluate quotation, the Purchaser may consider the following: (a) the Price as quoted; (b) price adjustment for correction of arithmetical errors; (a) Price adjustment due to discounts offered. 16.3 The Purchaser's evaluation of a quotation may require the consideration of other factors, in addition to the Price quoted if stated in Section II, Data Sheet. These factors may be related to the characteristics, performance, and terms and conditions of purchase of the Goods.
17. Purchaser's Right to Accept any Quotation, and to Reject any or all Quotations	17.1 The Purchaser reserves the right to accept or reject any quotation, and to annul the process and reject all quotations at any time prior to acceptance, without thereby incurring any liability to bidders.

F: Award of Contract	
18. Acceptance of the Quotation	18.1 The Purchaser will accept the quotation of the vendor whose offer has been determined to be the lowest evaluated bid and is substantially responsive to the documents issued.
19. Notification of acceptance	19.1 Prior to the expiration of the period of validity of quotation, the Purchaser will notify the successful vendor, in writing, that its quotation has been accepted.
20.Bid security	20.1 The bidder shall furnish as part of its bid, a Bid security (a) Be submitted in its original form; copies will not be accepted. (b) Bid security shall be valid up to **17th July 2025** (88) Days from the bid Closing data) (c) The amount of the bid security shall be sum total of the following amounts corresponding to individual items of the quotation and subjected to a maximum of Sri Lankan Rupees **10,000/=.**
21. Performance Security	21.1 Within twenty eight (28) days of the receipt of notification of award from the purchaser the successful Bidder if required shall furnish the Performance Security. The Performance Security form included in section V. The purchaser shall promptly notify the name of the winning bidder to each unsuccessful Bidder and discharge the bid securities of the unsuccessful bidders. 21.2 Failure of the successful Bidder to submit the above mentioned Performance Security shall constitute sufficient grounds for the amendment of the award and for failure of the Bid Security.
22. Payment Terms	**1st Milestone Payment**: **40%** of contract sum after the delivery of the 380 no's of Virus Software **2nd Milestone Payment**: **20%** of Initial contract sum after completing the installation and necessary trainings related to the software to IT staff. **3rd Milestone Payment**: **40%** of Initial contract sum after completing the parallel Run (21 Days) with the

	existing system and attending necessary user requirements by the contractor.

Section II: Data Sheet

ITV Clause Reference	
1.1	The Purchaser is : **Sri Lanka Land Development Corporation** Address: No. 3, Sri Jayawardenapura Mawatha, Welikada, Rajagiriya
2.2	A complete set of Bidding Documents in English language could be inspected and purchased upon submission of a written request to the Deputy General Manager (Supplies & Stores), on working days from **02/04/2025** to **21/04/2025** during 9.00 Hrs. to 15.30 Hrs. upon payment of non-refundable fee of **Rs 500/=** The method of payment will be in cash only.
5.1	If the bidder is allowed to quote for less than the all the items specified, indicate The details. - Evaluation shall be done separately. Kindly quote accordingly.
7.3	Manufacture's Authorizations required for Equipment's
11.1	Address for submission of Quotations is ***Chairman - Procurement Committee,*** ***Sri Lanka Land Development Corporation,*** ***No. 3, Sri Jayawardenapura Mawatha, Welikada, Rajagiriya*** Deadline for submission of quotations is Date: **22nd April 2025** Time: ***13.30 Hours***
13	The quotations shall be opened at the following address: ***Sri Lanka Land Development Corporation*** ***No. 3, Sri Jayawardenapura Mawatha,*** ***Welikada, Rajagiriya*** Date: **22nd April 2025** Time: ***13.30 hours - immediately after closing of bids***

16	Other factors that will be considered for evaluation are (List and describe the Methodology): Price, stocks past performance, quality of goods offered. Will be the criteria for selection

Schedule of Requirements

Item No.	Description of Goods	Qty.	Unit	Final Destination	Transportation and any other services	Delivery Date	
						Required Delivery	Bidders offered Delivery Terms (Please Mention Agreed or not)
1	**Purchase of Computer and Server Virus Protection Software**	380	Nos.	SLLDC Head Office, Rajagiriya	Supplier should arrange free of charge delivery	within 7 days	

	Description	Compliance (YES/ NO)	Remarks
Part 1: General Requirements			
1.1	Product Name and Category (AV/EDR or XDR)		
1.2	Product Version		
Part 2: Eligibility Requirements			
2.1	Solution must commercially available and requires no further research or development and is part of an existing product line with a field-proven operational history (that is, it has not simply been tested in a laboratory or experimental environment).		
2.2	Solution should support a Cloud hosted model where the vendor provides the management infrastructure, operational monitoring, and upgrades.		
2.3	Interested parties MUST provide 24/7 technical support, including issue/problem reporting and assistance.		
2.4	Solution MUST seamlessly integrate with all leading Security Information & Event Management (SIEM) Solution. Interested parties shall submit details of any dependencies together with the proposal.		
2.5	Solution should be compliance with ISO, SOC (Security Operations Center) & PCI standards such as (27001, SOC 2 Type II, PCI DSS)		
2.6	The proposed solution should be a leader in the latest Gartner Magic Quadrant for Endpoint Protection Platforms (EPP)		
2.7	The proposed solution should have performed with more than 98% protection & detection and have done the detections with zero configurations changes and zero number of delayed detections according to the MITRE ENGENUITY ATT&CK latest evaluation.		
2.8	Interested Parties shall indicate the adequate Skilled Human Resource availability to successfully complete the project within the agreed timeline.		
2.9	The proposed solution should provide more than 98% of sub-steps blocked according to the latest MITRE ENGENUITY ATT&CK Evaluation report.		
2.10	The proposed solution should provide more than 98% of technical level detections evaluated in the		

	MITRE ENGENUITY ATT&CK Evaluation in the latest report.		
2.11	The proposed solution should be a leader in the latest Forrester Wave report for Extended Detection and Response Platforms.		
2.12	The proposed solution shall run on a Single Agent (compatible for **Windows 7/10 and 11, Windows Server 2016 or upper with Full utilized SQL server 2017, Mac, and Linux OS**) and Single Console to reduce complexity.		
2.13	Proposed solution should be deployed and already in operation in at least 3 well-known organizations in Sri Lanka.		
2.14	Proposed solution must have at least one reference where solution is deployed and operational with at least 5,000 endpoints in Sri Lanka.		
2.15	The Bidder should have at least one customer reference for the proposed solution where the proposed solution is deployed with at least 4,000 endpoints in Sri Lanka.		
2.16	Proposed solution deployment and updates (agent, policies, settings, etc..) are available globally and where possible should not require forced rebooting during installation/upgrade without degrading performance of the proposed Endpoint Detection & Threat Prevention solution and the respective endpoint.		
Part 3: Endpoint Protection & Response General Requirements			
3.1.	The proposed solution must be tamper-resistant and protect endpoint sensors against attempts to modify.		
3.2.	Proposed solution must continuously collect data on all the entities and their activities within the environment such as: ○ File interaction – create, open, rename, delete, execute. ○ Process execution (including process tree). ○ User login. ○ Network traffic. ○ Registry changes. ○ Installed software.		
3.3.	The proposed solution must support the display of entity and activity data. Search behavioral patterns in all fields of coverage (users, files, machines, network traffic).		

3.4.	The solution shall be able to easily identify the root cause of a security event.		
3.5.	Proposed solution must support cross-organization queries. Search for the occurrence of process, file, network, or user activities across all endpoints.		
3.6.	Proposed solution must support: • Investigation of running processes or files. • Machine-level investigation.		
3.7.	Solution should have an evasion resistant virtual environment in which previously unknown file submissions are detonated to determine real-world effects and behavior.		
3.8.	The solution should provide a visual process tree browser for detected threats.		
3.9.	Solution should provide the option to mark discovered incidents as threats or duplicate threats.		
3.10.	Solution should support mechanism to define and assign various levels of security analysts automatically and manually based on detected incident criteria such as severity, host IP & port, username & domain.		
3.11.	Ability for an analyst to add notes/comments to an event.		
3.12.	Ability to notify assigned analysts of the incident via multiple communication methods such as email, slack and syslog.		
3.13.	Options to set the status of an issue or event (i.e., resolved, in progress, unresolved) or similar workflow.		
3.14.	Proposed solutions must support isolation and mitigation of malicious presence and activity globally across the entire environment.		
3.15.	Alert data related to threat detections should be available in the Management Console for at least about 6 months.		
3.16.	The proposed solution must support real-time dynamic identification and analysis of malicious content to detect and prevent zero-day attacks. (**These data should be available for minimum of 30 days**) and should be accessible through the dashboards for other investigations, regardless of the device state (online or offline)		

	For example, • Local IP address of the endpoint. • Logged in User ID with timestamps. • All process & service execution including admin tools and CMD commands. • All PowerShell Activities on endpoint • Suspicious File Activities (Zip, RAR & Scripts written). • Removeable Media Usage • Registry Edits. • Network listening ports on endpoints. • Network connections details.		
3.17.	The proposed solution must include a proactive cybersecurity approach that involves actively searching for and identifying unknown or ongoing cyber threats within SLLDC network.		
3.18.	The proposed solution must provide encrypted communication between the central EDR/XDR (Extended Detection and Response) management console and the agents on the endpoints or servers.		
3.19.	EDR/XDR agents should be able to leverage the OEMs threat intelligence database to prevent previously seen unknown malware.		
3.20.	The agent should be able to configure proxy parameters to ensure communication through a web proxy.		
3.21.	The solution should have a mechanism to collect logs centrally and forward them to the EDR tenant securely and efficiently instead of sending them directly from individual endpoints.		
3.22.	The solution should support high availability and redundancy for the log collector to ensure continuous operation.		
3.23.	The centralized log collector that comes with the proposed solution must be secure and hardened.		
3.24.	Proposed solution must support isolation and mitigation of malicious presence and activity on the endpoint, via remote operations, including and not limited to: I. Ability to run a coordinated command (such as CMD/PowerShell interface). II. Running scripts such as Perl/Python/Ruby or files from a network location or mapping a drive.		

	III. Isolating an endpoint or server from the network. IV. Deleting individual file, folders and exe (including active run files). V. Quarantine a file (including active run files). VI. Kill a process.		
3.25.	Proposed solution must support incident response automation (such as, incident custom rules for common scenarios available off-the-shelf as part of the solution and ability to define customized response workflows).		
3.26.	Solution custom detection rules should trigger automated workflows.		
3.27.	The solution must enable users to filter, sort, and aggregate incident data for efficient analysis, allowing quick identification of security issues and speeding up investigations with additional host context.		
3.28.	Solution must have filter options such as **incident id, status, severity, MITRE TTPs, host, detection sources**, etc for convenience of incident data analysis		
3.29.	The proposed solution should enable the integration of 3rd party security solutions through API (Application Programming Interfaces).		
3.30.	The proposed solution should have pre-built 3rd party integrations out-of-the-box.		
3.31.	The proposed solution should detect authentication spamming, brute force, attempt same password for many accounts and excessive logins through single agent and without the introduction of additional licenses or costs.		
3.32.	Should detect irregularities at attempting resource access using single agent without additional licensing or costs.		
3.33.	Should have visibility of active directory environment and identify potentially malicious account activity.		
3.34.	The proposed solution should be able to detect the most amount of attack sub-steps and prevent malware, evasive and zero-day threats with minimal configuration changes. Please provide independent 3rd party documentation for evidence.		
3.35.	Proposed solution should be able to track adversary Techniques, Tactics & Procedures. The		

	details of adversary, Tactics, Techniques, and Procedures (TTP)s should be available in the management console.		
3.36.	The proposed solution should have an in-built mechanism to initiate secure remote session for real-time response.		
Part 4: Endpoint Detection & Threat Prevention Capabilities and Features			
4.1.	Solution shall have machine learning capabilities and the ability to detect and block malicious files without relying on daily/weekly definition updates.		
4.2.	The proposed solution shall be able to detect file less attack and script base attack without using signatures and automatically kill the process based on policy settings.		
4.3.	The solution shall use algorithms to prevent malware.		
4.4.	Solution should be able to detect known threats by analyzing the characteristics of samples file prior to execution.		
4.5.	The solution should protect the endpoint against malware, even when the system is not connected to the network and respond appropriately to sophisticated threats in real time.		
4.6.	The solution must find and eradicate threats across endpoints, allowing real-time scanning and elimination of malicious files anywhere in the environment		
4.7.	The solution must provide automated and manual mechanisms to find and eradicate detected threats and artifacts across all endpoints.		
4.8.	The solution shall have the capability to quarantine unknown and zero-day malware.		
4.9.	The solution should leverage Artificial Intelligence or Machine Learning to analyze files pre-execution.		
4.10.	The solution should have the capability to forward unknown files to a cloud to further analyze.		
4.11.	Supports analysis of a broad range of file types, including executable programs, Microsoft Office files, Dynamic link (.dill), (APK) files etc. and should support file sizes up to 100MB		
4.12.	The proposed solution should be able to do dynamic unpacking and to identify and unpack		

	files that have been encrypted using custom/open-source methods for the analysis.		
4.13.	The solution should leverage Artificial Intelligence or Machine Learning to analyze behaviors while a file is running.		
4.14.	The proposed solution must identify malicious files and prevent them from execution, including viruses, trojans, ransomware, spyware, and crypto miners using machine learning and behavioral techniques before it could create any damage to respective systems.		
4.15.	Proposed solution must identify malicious behavior of executed files, running processes, registry modifications, or memory access and terminate them at runtime.		
4.16.	The solution must enable the enforcement of host-based firewall policy on organization endpoints, allowing control over communications and providing visibility into network connections.		
4.17.	The solution host-based firewall must support the creation of different firewall rules within the host firewall policy, ensuring reusability across all host firewall profiles.		
4.18.	Should support single firewall rule to apply for multiple operating systems.		
4.19.	The solution must seamlessly integrate with the Windows Security Center, applying rules to devices. It should include a Host Firewall Events table for easy tracking of enforcement activities across the organization.		
4.20.	Should enforce different rules when the endpoint is located within the organization's internal network, and when it is outside.		
4.21.	Proposed solution should have mechanism to provide identity hygiene and proactive protection against identity-based attack threat landscape.		
4.22.	Proposed solution should provide insight into host and user risk view.		
4.23.	Solution proposed should detect & prevent MFA spamming.		
4.24.	Solution should prevent against brute force, password spray, and excessive logins.		
4.25.	The proposed solution must identify and block/alert on lateral movement		
4.26.	Proposed solution should have UEBA module which utilizes machine learning and behavioral analysis in order to profile users and entities.		

4.27.	Solution UEBA should analyze and alert on behaviors that are anomalous and suspicious that may indicate compromised account or malicious insider through single agent architecture and without the inclusion of additional licenses or costs.		
4.28.	Solution UEBA systems should gather comprehensive data, including user activities, network traffic, and access logs, etc, to enable the creation of a baseline and to analyze user behavior through single agent and without the introduction of supplementary licenses or additional costs.		
4.29.	Solution should ensure no performance impact for Business-Critical Applications of the customer (SAP B1, IMS, Zimbra Email etc.)		
4.30.	CPU Utilization should be lower than 2%		
4.31.	Memory utilization should be lower than 150MB		
Part 5: XDR Requirements			
5.1.	Proposed solution should support XDR capabilities for 3rd party log ingestion for future integration requirements.		
Part 6: Device Control Features			
6.1.	Solution should include the capability to manage and control the use of USB peripheral devices. (Allow Read & Write, Read Only, Block)		
6.2.	Solution device control should provide easy configuration to allow blocked USB devices through device activity logs.		
6.3.	Solution device control should include the capability to manage and control access of both Bluetooth devices and Low Energy Bluetooth devices (Allow, Block)		
6.4.	Proposed solution device control should provide device control to be implemented through multiple device definition levels such as device id, device family, device type etc.		
6.5.	Proposed solution device control should log device activity of allowed and blocked devices.		
6.6.	Solution must provide the USB device control management, configuration, and visibility from the same single console.		
6.7.	Solution should provide USB device control policies based on endpoints, host IP address & ranges, host name, domain and username.		
6.8.	Proposed solution should include mechanisms to manipulate embedded hardware modules such		

	as (Wireless, Bluetooth, etc) to disable, enable and stop.		
6.9.	Proposed solution should have capability to enable and manage disk encryption of endpoints using native-full volume encryption features (ex: BitLocker, FileVault)		
6.10.	Proposed solution should enable and manage full disk and partial disk encryption.		
Part 7: Vulnerability Management			
7.1.	The proposed solution should have a built-in vulnerability assessment scanner to discover vulnerabilities related to operating system and installed 3rd party applications.		
7.2.	The proposed solution's OS and application vulnerability assessment scanner module should provide filtering of the identified vulnerabilities based on OS, Machine Type, etc.		
7.3.	The proposed solution should have real-time visibility into vulnerability exposure and current patch levels in endpoints for both OS level and 3rd party applications vulnerabilities.		
7.4.	The proposed solution OS and application vulnerability assessment scanner module should map the discovered vulnerabilities to the specific CVE ID.		
7.5.	Vulnerability Management module monitoring and visibility from the same single console.		
Part 8: Agent Features			
8.1.	Use of signature-less algorithm to detect and prevent malware.		
8.2.	Use of AI/ML powered Static and Behavioral analysis to detect and prevent a wide range of attacks in real time.		
8.3.	Solution should support Intelligent Run-time Memory Analysis with advanced detectors used to analyze modern threats utilizing a multitude of evasion techniques.		
8.4.	Ability to enable on-demand scanning and to configure scheduled-scanning for all endpoints.		
8.5.	Host-based firewall controller to control network connectivity.		
8.6.	Ability to discover unmanaged and unprotected endpoints.		
8.7.	Application vulnerability scanner for both OS and application inventory vulnerability mapping.		

8.8.	Agent should have User and Entity Behavior Analytics (UEBA) module which establishes a baseline and profiles users based on behaviors.		
8.9.	Agent protection should be available even though endpoint resources get exhausted due to sudden hardware resource requirement spikes.		
8.10.	Agent should also encompass security features that enable identity hygiene and help detection and protection of identity-based attacks.		
Part 9: Operating System Platform Support			
9.1.	Agent should support the deployment to the following Windows Clients versions: • Windows 7 • Windows 10 (Update 22H2) • Enterprise and Professional Updates 21H2, 21H1, 20H2, 2004, 1909, 1809 • Windows 10 -Enterprise 2019 LTSC • Windows 10 IoT (Internet of Things) Core • Windows 10 IoT Enterprise • Windows 11 - Update 24H2 / Update 23H2 / Update 22H2 / Pro /Pro Education /Pro Workstations / Enterprise / Education / Home / IoT Enterprise		
9.2.	Agent should support the deployment to the following Windows versions: • Windows Server Core 2012, 2012 R2, 2016, 2019, and 2022 • Windows Server 2025, 2022, 2019, 2016, 2012 R2, 2012		
9.3.	Agent support for the following virtual application & environments &: • VMware AppVolumes • VMware ESXi VM • VMware Workstation VM • VMware Horizon • VMware ThinApp • Microsoft Hyper-V • Windows Virtual PC • Vcenter		
9.4.	Agent support for mobile devices: • Android 8 and later • iOS 15.0 and later		
9.5.	Agent support for the following Linux environments: • CentOS (6.7+, 7.0-7.9, 8.0-8.3, 8.4, 9) • Ubuntu 12.04 / 14 / 16 / 18 / 20/ 22 / 24		
Part 10: Operations & Policy Management			

10.1.	Proposed solution is fully manageable via Central Cloud Console Administrator.		
10.2.	Proposed solution management console must enable the set up & push policies, run tasks, collect logs, and get notifications and an overall security overview of the network via a central web-based management console.		
10.3.	Proposed solution must have a light footprint for minimal impact on the endpoint/server performance. Indicate the expected maximum RAM, CPU, Bandwidth consumption etc.		
10.4.	Proposed solution must provide policy and rule set up & configuration for mobile endpoints from same unified single console.		
10.5.	Proposed solution management console should notify administrators of risky and unsafe policies at the time of creation of policies.		
Part 11: Central Cloud Management Console			
11.1.	The solution should provide a web-based console that allows administrators to access the management interface from any machine.		
11.2.	The proposed solution must provide capability to only allow tenant access to authorized users with approved IP addresses and domains.		
11.3.	Management console should provide granular role-based access to a tenant to enable role delegation and structured management of endpoints.		
11.4.	Solution should provide updates and console connectivity through a separate dedicated proxy server for closed environments that do not have direct outbound connectivity.		
11.5.	Solution should provide through the management console, convenient integration & console connectivity settings for the dedicated proxy server, to update content of endpoints for such closed environments.		
11.6.	Solution should provide convenient management of configuration changes of parameters for the proxy server through the management console without the use of scripts or having to repackage agent.		
11.7.	Solution should provide secure communication and connectivity with the management console for both outbound and inbound.		
11.8.	Centrally collect and process alerts in real-time.		

11.9.	The solution should have centralized policy management and reporting architecture that can scale on a single console.		
11.10.	Proposed solution should provide capability to select the datacenter location of the management console and have custom management console URL at tenant activation.		
11.11.	Proposed solution management console should provide ability to crate aggregated security rules for host-based firewall, device control and disk encryption in a single consolidated policy.		
11.12.	Management console should have list of pre-built dashboard widgets with the ability to create customer widgets based on pre-existing widgets and query-based widgets for fully customizable widgets.		
11.13.	Management console should have list of pre-defined reports and should also provide mechanism to create fully customizable reports based on both pre-defined reports and query-based reports.		
11.14.	The proposed solution must support connection to Active Directory.		
11.15.	Solution should have the option to provide dynamic policy assignment based on device attributes and usernames.		
11.16.	Policy modifications should be applied in near real time.		
11.17.	Specify a schedule for downloading updates, with the ability to disable automatic updates.		
11.18.	Provide mechanism to stage the agent update process to endpoints in a test environment prior to being deployed in the production environment.		
11.19.	Solution should provide ability to cache agent update in order to facilitate agent update control and test environment staging.		
11.20.	Solution agent update control mechanism should provide agent update automation capabilities in order to automate agent update workflow and deployment (for example staging environment will always have latest version “n” while production environment shall maintain version “n-1”)		
11.21.	Support integration with email infrastructure to notify security personnel in case of alerts.		
11.22.	Proposed solution shall provide log collection, retention, and integration with SIEM.		

11.23.	Management console should provide the ability to specify user account inactive time period for administrators to disable access for the management console.		
Part 12: Managed Detection & Response (MDR)			
12.1.	Managed Detection & Response Services (MDR) should provide 24/7 manage detection and response service to effectively manage threats.		
12.2.	Solution should include 24/7 proactive threat hunting service to avoid possible zero-day attacks, APT attacks etc.		
12.3.	The proposed MDR services should have the capability to provide 24x7 monitoring and investigation of alerts.		
12.4.	MDR service provided must perform an in-depth root cause analysis to provide an understanding of how the attack was initiated, spread, and which devices were affected.		
12.5.	Solution should support 24/7 managed threat hunting for detection of hidden, stealthy attacks and hands on activities.		
12.6.	Proposed MDR service should at least have 3 references where MDR services are provided for critical operations.		
Part 13: Support & Services			
12.7.	Should provide 1 year 24 x 7 support through an OEM certified service support center located locally within Sri Lanka.		
12.8.	The proposed vendor or authorized agent should have a certified authorized 24/7 technical support center in Sri Lanka, which includes support via phone, email, and remote assistance which operates with certified engineers.		Proof Documents shall be submitted

LIST OF PAST PROJECTS COMPLETED

(Provide three(03) similar type sales for organizations, value over Rs.250,000 completed during past 18months)

No.	Name of the Project	Number of Anti-Virus installed	Client/ Contact No.	Contract Value (Rs)	Date of Completion
1					
2					
3					

……Signature
and the Seal of Bidder

Bill of Quantities

No	Description	Qty	Warranty	Unit Price (LKR)	Total (LKR)
01	End Point Detection and Response (EDR) Software License (**1 Year License and Support, should comply with all the features mentioned under the specifications**)	380	1 Year		

Discount if any (Less)	
Total Price before VAT(LKR)	
VAT (LKR)	
Total Amount (LKR)	

Amount in words	
Company Name	
Address	
Witness Name, NIC and Signature	
Company Seal Name	

Mandatory Requirement that shall be fulfilled by the vender

No	*Description*	*Supplier Specification or Or, Agreed, Attached document*
1	*Company Registration - BR*	
2	*Bidder shall provide all the necessary technical support within the warranty period*	
3	*Maintenance services Under warranty Period specify*	
4	*After receiving the P.O you have to deliver the goods to SLLRDC Within 07 days*	
5	*Submit the Manufacture Certificates & Authorization Certificates for the Product*	
6	*At least 5 years' experience in the field.*	
7	*Technical support shall be Provide with 06 Hours or less after logging the Job*	
8	*Please Attached Company engineer or employed details*	
9	*2023/24 Gartner Magic Quadrant and Forrester Wave report for Endpoint Protection Platforms shall be submitted*	

Section V

Quotation Submission Form

[The Vendor shall fill in this Form in accordance with the instructions indicated. No Alterations to its format shall be permitted and no substitutions will accepted.]

Date:……

To: *[insert complete name of Purchaser]*……

……

We, the undersigned, declare that:

(a) We have examined and have no reservations to the document issued;

(b) We offer to supply in conformity with the documents issued and in accordance with the Delivery Schedules specified in the Schedule of Requirements the following Goods ……..*[insert a brief description of the Goods];*

(c) The total price of our quotation including any discounts offered is: ……..*[insert the total quoted price in words and figure];*

(d) Our quotation shall be valid for the period of time specified in ITV Sub-Clause 8.1, from the date fixed for the quotation submission deadline in accordance with ITV Sub-Clause 11.1, and it shall remain binding upon us and may be accepted at any time before the expiration of that period;

(e) We understand that this quotation, together with your written acceptance thereof included in your notification of award, shall constitute a binding contract between us.

(f) We understand that you are not bound to accept the lowest evaluated quotation or any other quotation that you may receive.

Signed: *[insert signature of person whose name and capacity are shown]*

……

Name: *[insert complete name of person signing the Bid Submission Form]*

……

Dated:

Bid Security (Bank Guarantee)

[The Bank shall fill in this Bank Guarantee Form in accordance with the instructions indicated.]

_____

[Bank's Name, and Address of Issuing Branch or Office]

Beneficiary: _____ *[Name and Address of Purchaser]*

Date: _____

BID GUARANTEE No.: _____

We have been informed that *[name of the Bidder]* (hereinafter called "the Bidder") has submitted to you its bid dated (hereinafter called "the Bid") for the execution of *[name of contract]* under Invitation for Bids No. *[IFB number]* ("the IFB").

Furthermore, we understand that, according to your conditions, bids must be supported by a bid guarantee.

At the request of the Bidder, we *[name of Bank]* hereby irrevocably undertake to pay you any sum or sums not exceeding in total an amount of *[amount in figures]* (*[amount in words]*) upon receipt by us of your first demand in writing accompanied by a written statement stating that the Bidder is in breach of its obligation(s) under the bid conditions, because the Bidder:

(a) has withdrawn its Bid during the period of bid validity specified by the Bidder in the Form of Bid; or

(b) having been notified of the acceptance of its Bid by the Purchaser during the period of bid validity, (i) fails or refuses to execute the Contract Form; or (ii) fails or refuses to furnish the performance security, if required, in accordance with the Instructions to Bidders.

This guarantee will expire: (a) if the Bidder is the successful bidder, upon our receipt of copies of the contract signed by the Bidder and the performance security issued to you upon the instruction of the Bidder; or (b) if the Bidder is not the successful bidder, upon the earlier of (i) our receipt of a copy of your notification to the Bidder of the name of the successful bidder; or (ii) twenty-eight days after the expiration of the Bidder's Bid.

Consequently, any demand for payment under this guarantee must be received by us at the office on or before that date.

This guarantee is subject to the Uniform Rules for Demand Guarantees, ICC Publication No. 458.

_____

[signature(s)]

Manufacturer's Authorization

[If requested under ITV clause 7.3, the Bidder shall require the Manufacturer to fill in this Form in accordance with the instructions indicated.]

Date:

WHEREAS

We *[insert complete name of Manufacturer],* who are official manufacturers of *[insert type of goods manufactured],* having factories at [insert full address of Manufacturer's factories], do hereby authorize *[insert complete name of Bidder]* to submit a quotation the purpose of which is to provide the following Goods, manufactured by us *[insert name and or brief description of the Goods],* and to subsequently negotiate and supply the goods.

We hereby extend our full guarantee and warranty, with respect to the Goods offered by the above firm.

Signed: *[insert signature(s) of authorized representative(s) of the Manufacturer]*

Name: *[insert complete name(s) of authorized representative(s) of the Manufacturer]*

Title: *[insert title]*

Duly authorized to sign this Authorization on behalf of: *[insert complete name of Bidder]*

Dated on_____day of_____,_____*[insert date of signing]*

Performance Security

[The bank, as requested by the successful Bidder, shall fill in this form in accordance with the instructions indicated]

Date: *[insert date (as day, month, and year) of Bid Submission]*

Procurement No.: ***S/105/25***

Purchase of Computer and Server Virus Protection Software for SLLDC Head Office

Bank's Branch or Office: *[insert complete name of Guarantor]*

Beneficiary: **General Manager,**
Sri Lanka Land Development Corporation
Ministry of Urban Development, Water supply and Housing facilities

PERFORMANCE GUARANTEE No.: *[insert Performance Guarantee number]*

We have been informed that *[insert complete name of Supplier]* (hereinafter called "the Supplier") has entered into Contract No*. [insert number]* dated *[insert day and month], [insert year]* with you, for the supply of *[description of Goods]* (hereinafter called "the Contract").

Furthermore, we understand that, according to the conditions of the Contract, a Performance Guarantee is required.At the request of the Supplier, we hereby irrevocably undertake to pay you any sum(s) not exceeding *[insert amount(s[1]) in figures and words]* upon receipt by us of your first demand in writing declaring the Supplier to be in default under the Contract, without cavil or argument, or your needing to prove or to show grounds or reasons for your demand or the sum specified therein.This Guarantee shall expire no later than the *[insert number]* day of *[insert month][insert year]*,[2] and any demand for payment under it must be received by us at this office on or before that date.This guarantee is subject to the Uniform Rules for Demand Guarantees, ICC Publication No. 458, except that subparagraph (ii) of Sub-article 20(a) is hereby excluded.

---

[1] *The Bank shall insert the amount(s) specified in the SCC and denominated, as specified in the SCC, either in the currency(ies) of the Contract or a freely convertible currency acceptable to the Purchaser.*

[2] *Dates established in accordance with Clause 18.4 of the General Conditions of Contract ("GCC"), taking into account any warranty obligations of the Supplier under Clause 16.2 of the GCC intended to be secured by a partial Performance Guarantee. The Purchaser should note that in the event of an extension of the time to perform the Contract, the Purchaser would need to request an extension of this Guarantee from the Bank. Such request must be in writing and must be made prior to the expiration date established in the Guarantee. In preparing this Guarantee, the Purchaser might consider adding the following text to the Form, at the end of the penultimate paragraph: "We agree to a one-time extension of this Guarantee for a period not to exceed [six months] [one year], in response to the Purchaser's written request for such extension, such request to be presented to us before the expiry of the Guarantee."*

. . . . . *[signatures of authorized representatives of the* ***Bank and the Supplier]***