ELCOT
Adding Value through IT

Electronics Corporation of Tamil Nadu Limited

Corrigendum

Corrigendum No.1 to the Tender Document for the

Tender To Supply, Installation and Commissioning of Linux Enterprise Server Operating System& Antivirus with HIPS features for TNeGA

Tender Ref.

ELCOT/Proc/OT/33496/ Linux Enterprise Server Operating System & Anti Virus for TNeGA /2021-22

Electronics Corporation of Tamil Nadu Limited
MHU Complex II Floor,
692 Anna Salai, Nandanam
Chennai-600035
Phone: +91-44-66401400 Fax: +91-44-2433 0612
Email: proctenders@elcot.in Website: www.elcot.in

CORRIGENDUM TO THE TENDER DOCUMENT

The following Corrigendum to the Tender Document is hereby issued:-

S.N	Title of the clause	Existing	To be read as
1.	Page No. 9– Tender Schedule Point No. 2 - (6) Tender Schedule & Earnest Money Deposity(EMD)	**Rs.50,000/- (Rupees Fifty Thousand only)** should be paid electronically through the Bidder's respective internet banking enabled account via NEFT / RTGS to the account of ELCOT: **Account Number: 6681528770** **Indian Bank, Nandanam Branch, Chennai – 600 035.** **IFSC Code: IDIB000N078.**	**Rs.50,000/- (Rupees Fifty Thousand only)** should be paid electronically through the Bidder's respective internet banking enabled account via NEFT / RTGS to the account of ELCOT: **Account Number: 6681528770** **Indian Bank, Nandanam Branch, Chennai – 600 035.** **IFSC Code: IDIB000N078.** The bidder seeking EMD exemption for MSME/NSIC/SSI, must submit the valid supporting document for the relevant category. Units having either permanent SSI Registration Certificate prior to implementation of MSMED Act, 2006 or valid Entrepreneurs Memorandum Part-II issued by the Directorate of Industries & Commerce or UdyogAadhar Memorandumare exempted from payment of EMD. The tenders without Earnest Money Deposit or Valid MSME/NSIC/SSI certificate / UdyogAadhar for exemption of EMD will be summarily rejected

Addendum to the Specification of Antivirus with HIPS feature – 33496-002

Make : To be specified

S.No.	Minimum Specifications	Bidder Compliance (Yes/No)	Product Compliance (Yes/No)
1	The solution must provide single platform for complete server protection over physical, virtual (server) & cloud and should protects mainly Linux platforms.		
2	The proposed solution provides self-defending servers; with multiple integrated modules below providing a line of defence at the server in a single agent: Anti-virus/Anti-malware, HIPS, Application control, Log Inspection, File Server protection, vulnerable software patching, anti-ransomware.		
3	The Proposed Solution should Support Realtime monitoring and should be able to detect and clean malware even if it is stagnant and not executing		
4	The proposed solution must be able to perform machine learning to discover new threats before file is executed and able to monitor behaviour of running process to detect malicious behaviour		
5	The proposed Solution should support Scan Cache for better performance		
6	Must be able to provide scan assessment engine to discover OS & application vulnerabilities on a server and determine which vulnerabilities have not been mitigated & recommend rules to shield applications & systems with advanced deep packet inspection technology		
7	Must be able to operate in detection or prevention mode to protect operating systems and enterprise application vulnerabilities.		
8	Solution should provide layered defence against advanced attacks and shields against known and unknown vulnerabilities in web and enterprise applications and operating systems.		
9	Must be able to provide Application Control in whitelist or blacklist mode		
10	The solution should support Maintenance Mode in which during predefined Downtimes, upgrade etc can take place and all processes automatically learnt and Whitelisted		
11	Must be able to monitor critical operating system and application such as directories, registry keys, and values to detect and report malicious and		

	unexpected changes in real-time		
12	The proposed solution should have intelligence to analyse and share key informational log events for correlation to SIEM		
13	The solution must support integration with leading SIEM systems using syslogs, CEF and LEEF Format		
14	The proposed solution should be positioned in the leader quadrant from last three published Gartner Magic quadrant report for Endpoint Protection		

General Manager (Proc)(FAC)