Anexa nr. 2

Formularul ofertei pentru bunuri şi servicii

Data depunerii ofertei: „28” august 2023

Procedura de achiziție Nr.: ocds-b3wdp1-MD-1691570951766 (72200000-7)

Anunț de participare Nr.: 60

Către: ÎNTREPRINDEREA DE STAT POŞTA MOLDOVEI

Î.M. “Orange Moldova” S.A. declară că:

a) Au fost examinate şi nu există rezervări faţă de documentele de atribuire, inclusiv modificările nr. nu au fost modificari.

b) Î.M. “Orange Moldova” S.A. se angajează să presteze, în conformitate cu documentele de atribuire şi condiţiile stipulate în specificaţiile tehnice şi preţ, următoarele: **Software Antivirus.**

c) Suma totală a ofertei fără TVA constituie: **245,625.00** (două sute patruzeci şi cinci mii şase sute douăzeci şi cinci.00) MDL.

d) Suma totală a ofertei cu TVA constituie: **294,750.00** (două sute nouăzeci şi patru mii şapte sute cincizeci.00) MDL.

e) Prezenta ofertă va rămîne valabilă pentru perioada de timp 60 zile, începînd cu data-limită pentru depunerea ofertei, în conformitate cu **Anexa 22. şi Anexa 23**, va rămîne obligatorie şi va putea fi acceptată în orice moment pînă la expirarea acestei perioade;

f) Compania semnatară, afiliaţii sau sucursalele sale, inclusiv fiecare partener sau subcontractor ce fac parte din contract, nu au fost declarate neeligibile în baza prevederilor legislaţiei în vigoare sau a regulamentelor cu incidenţă în domeniul achiziţiilor publice.

Data completării 28.08.2023

Cu stimă,
Anatolie Bulgaru
Head of B2B IoT and ICT
Î.M. „Orange Moldova” S.A.
Acest act este semnat prin aplicarea Semnăturii Mobile
Verificarea semnăturii - https://msign.gov.md/#/verify/upload

Anexa nr.1

Specificația tehnică pentru software antivirus.

№	Requirement	Compliance (Yes/No)	Comment
System requirements			
1.	**The proposed solution must support the operating systems below:** • Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 or later • Windows 8 Professional / Enterprise • Windows 8.1 Professional / Enterprise • Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise • Windows 11 **Servers** • Windows Small Business Server 2011 Essentials / Standard (64-bit) • Windows MultiPoint Server 2011 (64-bit) • Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 or later • Windows Server 2012 Foundation / Essentials / Standard / Datacenter • Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter • Windows Server 2016 Essentials / Standard / Datacenter • Windows Server 2019 Essentials / Standard / Datacenter • Windows Server 2022 **Microsoft Terminal Servers** • Microsoft Remote Desktop Services based on Windows Server 2008 R2 SP1 • Microsoft Remote Desktop Services based on Windows Server 2012 • Microsoft Remote Desktop Services based on Windows Server 2012 R2 • Microsoft Remote Desktop Services based on Windows Server 2016 • Microsoft Remote Desktop Services based on Windows Server 2019 **32-bit Linux operating systems:** • CentOS 6.7 and later • Debian GNU / Linux 9.4 and later • Debian GNU / Linux 10.1 and later • Linux Mint 19 and later • Mageia 4 • Red Hat Enterprise Linux 6.7 and later • ALT Education 9 • ALT Workstation 9 • ALT Server 9 **64-bit Linux operating systems:** • AlterOS 7.5 and later • Amazon Linux 2 • Astra Linux Common Edition (operational update 2.12). • Astra Linux Special Edition RUSB.10015-01 (operational update 1.5) • Astra Linux Special Edition RUSB.10015-01 (operational update 1.6) • Astra Linux Special Edition RUSB.10015-16 (release 1) (operational update 1.6) • CentOS 6.7 and later • CentOS 7.2 and later • CentOS 8.0 and later • Debian GNU / Linux 9.4 and later • Debian GNU / Linux 10.1 and later • EulerOS V2.0SP2 2.2.17	**Yes**	Antivirus Licenses: Kaspersky Endpoint Security for Business – Select/ Kaspersky Endpoint Detection and Response Optimum Add-on

	• EulerOS V2.0SP5 2.5.6 • Linux Mint 19 and later • Linux Mint 20.1 and later • openSUSE Leap 15.0 and later • Oracle Linux 7.3 and later • Oracle Linux 8.0 and later • Pardus OS 19.1 • Red Hat Enterprise Linux 6.7 and later • Red Hat Enterprise Linux 7.2 and later • Red Hat Enterprise Linux 8.0 and later • SUSE Linux Enterprise Server 12 SP5 and later • SUSE Linux Enterprise Server 15 and later • Ubuntu 18.04 LTS and later • Ubuntu 20.04 LTS • ALT Education 9 • ALT Workstation 9 • ALT Server 9 • GosLinux 7.2 • Red OS 7.3 **MAC OS operating systems:** • macOS 10.14 – 12		
2.	The proposed solution must support the following virtual platforms: • VMware Workstation 16.1.1 Pro • VMware ESXi 7.0 Update 2a • Microsoft Hyper-V Server 2019 • Citrix Virtual Apps and Desktops 7 2103 • Citrix Provisioning 2012 • Citrix Hypervisor 8.2 LTSR	**Yes**	
3.	The proposed solution must support protection of the latest Operating Systems versions across all platforms (Windows, Linux, MacOS, iOS, Android).	**Yes**	
Functional requirements			
2.1	**Functional requirements: Antivirus**		
	The proposed solution must be able to detect following types of threat: • Viruses (including polymorphic), Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, Phishing sites and links, Zero-Day Vulnerabilities and other malicious and unwanted software.	**Yes**	Antivirus Licenses: Kaspersky Endpoint Security for Business – Select/ Kaspersky Endpoint Detection and Response Optimum Add-on
	The proposed solution must support Anti-malware Scan Interface (AMSI).	**Yes**	
	The proposed solution must have the ability to integrate with Windows Defender Security Center.	**Yes**	
	The proposed solution must support Windows Linux subsystem.	**Yes**	
	The proposed solution must provide next gen protection technologies. For example: • protection against file-less threats • provision of multi-layered Machine Learning (ML) based protection and behavioral analysis during different stages of the kill-chain	**Yes**	
	The proposed solution must provide Memory Scanning for Windows workstations.	**Yes**	
	The proposed solution must provide Kernel Memory Scanning for Linux workstations.	**Yes**	
	The proposed solution must provide the ability to switch to cloud mode for threat protection, decreasing RAM and hard disk drive usage for resource-limited machines.	**Yes**	
	The proposed solution must have dedicated components to monitor, detect and block activities on Windows, Linux and Windows servers, and endpoints, to protect against remote encryption attacks.	**Yes**	
	The proposed solution must include signatureless components to detect threats even without frequent updates. Protection must be powered by Static ML for pre-execution and Dynamic ML for post-execution stages of the kill-chain on endpoints and in the cloud for Windows servers and workstations.	**Yes**	
	The proposed solution must provide behavioral analysis based on ML.	**Yes**	

	The proposed solution must provide the ability to integrate with the vendor's own Endpoint Detection and Response (EDR) and Anti-APT solutions, for active threat hunting and automated incident response.	**Yes**	
	The proposed solution must support integration with a standalone/independent automated threat detection and prevention sandbox solution that does not depend on the vendor's EDR and /or Anti-APT solution.	**Yes**	
	The proposed solution must include the ability to configure and manage firewall settings built into the Windows Server and Linux operating systems, through its management console.	**Yes**	
	The proposed solution must provide Application and Device Controls for Windows workstations.	**Yes**	
	The proposed solution's protection for servers and workstations must include a dedicated component for protection against ransomware/cryptor virus activity on shared resources.	**Yes**	
	The proposed solution must, on detecting ransomware/cryptor-like activity, automatically block the attacking computer for a specified interval and list information about the attacking computer IP and timestamp, and the threat type.	**Yes**	
	The proposed solution must provide a pre-defined list of scan exclusions for Microsoft applications and services.	**Yes**	
	The proposed solution should support the installation of endpoint protection on servers without the need to restart.	**Yes**	
	The proposed solution must enable the following for endpoints: • Manual Scanning • On-Access Scanning • On-Demand Scanning • Compressed File Scanning • Scan Individual File, Folder and Drive • Script Blocking and Scanning • Registry Guard • Buffer Overflow Protection • Background/Idle Scanning • Removable Drive Scanning on connection with system • The ability to detect and block untrusted hosts on detection of encryption-like activities on server shared resources.	**Yes**	
	The proposed solution should be password-protected to prevent the AV process being halted/killed and for self-protection, regardless of the user authorization level on the system.	**Yes**	
	The proposed solution must have both local and global reputation databases.	**Yes**	
	The proposed solution must be able to scan HTTPS, HTTP and FTP traffic against viruses and spyware, or any other malware.	**Yes**	
	The proposed solution must include a personal firewall capable, as an absolute minimum, of: • Blocking network activates of applications based on their categorization. • Blocking/allowing specific packets, protocols, IP addresses, ports and traffic direction. • The automatic and manual addition of network subnets, and modification of network activity permissions.	**Yes**	
	The proposed solution must prevent the connection of reprogrammed USB devices emulating keyboards, and enable control of the use of onscreen keyboards for authorization.	**Yes**	
	The proposed solution must be able to block network attacks and report the source of the infection.	**Yes**	
	The proposed solution must have local storage on endpoints to keep copies of files that have been deleted or modified during disinfection. These files must be stored in a specific format that ensures they cannot pose any threat.	**Yes**	
	The proposed solution must have a proactive approach to preventing malware from exploiting existing vulnerabilities on servers and workstations.	**Yes**	
	The proposed solution must support AM-PPL (Anti-Malware Protected Process Light) technology for protection against malicious actions.	**Yes**	

	The proposed solution must include protection against attacks that exploit vulnerabilities in the ARP protocol in order to spoof the device MAC address.	**Yes**	
	The proposed solution must provide Anti-Bridging functionality for Windows workstations to prevent unauthorized bridges to the internal network that bypass perimeter protection tools. Administrators should be able to ban the establishment of simultaneous wired, Wi-Fi, and modem connections.	**Yes**	
	The proposed solution must include a dedicated component for scanning encrypted connections.	**Yes**	
	The proposed solution must be able to decrypt and scan network traffic transmitted over encrypted connections supported by the following protocols; SSL 3.0, TLS 1.0, TLS1.1, TLS1.2, TLS 1.3.	**Yes**	
	The proposed solution must have the ability to automatically exclude web resources when a scan error occurs while performing an encrypted connection scan. This exclusion must be unique to the host and must not be shared with other endpoints.	**Yes**	
	The proposed solution must include functionality to remotely wipe data on the endpoint (for workstations).	**Yes**	
	The proposed solution must have following remote data wipe functionalities: • In silent mode • On hard drives and removable drives • For all user accounts on the computer	**Yes**	
	The proposed solution's remote data wipe functionality must support the following modes: • Immediate data deletion • Postponed data deletion	**Yes**	
	The proposed solution's remote data wipe functionality must support the following data deletion methods: • Delete by using the operating resources - files are deleted but are not sent to the recycle bin • Delete completely, without recovery - making data practically impossible to restore after deletion	**Yes**	
	The proposed solution must include functionality to automatically delete the data if there is no connection to the endpoint management server.	**Yes**	
	The proposed solution must support signature-based detection in addition to cloud-assisted and heuristics.	**Yes**	
	The proposed solution should have the ability to raise an alert on, clean, and delete a detected threat.	**Yes**	
	The proposed solution should have the ability to accelerate scanning tasks, skipping those objects that have not changed since the previous scan.	**Yes**	
	The proposed solution should have the ability to prioritize custom and on-demand scanning tasks for Linux workstations.	**Yes**	
	The proposed solution must allow the administrator to exclude specified files/ folders/applications/digital certificates from being scanned, either on-access (real-time protection) or during on-demand scans.	**Yes**	
	The proposed solution should include the functionality to isolate infected computers.	**Yes**	
	The proposed solution must automatically scan removable drives for malware when they are attached to any endpoint. Scan control should be based on drive size.	**Yes**	
	The proposed solution must be able to block the use of USB storage devices or allow access only to permitted devices, and allow read/write access only by domain users, to reduce data theft and enforce lock policies.	**Yes**	
	The proposed solution must be able to differentiate between USB storage devices, printers, mobiles and other peripherals.	**Yes**	
	The proposed solution must be able to log file operations (Write and Delete) on USB storage devices. This should not require any additional license or component to be installed on the endpoint.	**Yes**	
	The proposed solution must have ability to block the execution of any executable from the USB storage device.	**Yes**	
	The proposed solution must have ability to block/allow user access to web resources based on websites, content type, user and time of day.	**Yes**	
	The proposed solution must have a specific detection category to block website banners.	**Yes**	

	The proposed solution must provide the ability to configure Wi-Fi networks based on Network Name, Authentication Type, Encryption Type, so these can later be used to block or allow the Wi-Fi connections.	**Yes**	
	The proposed solution must support user-based policies for Device, Web and Application Control.	**Yes**	
	The proposed solution should specifically allow the blocking of the following devices: • Bluetooth • Mobile devices • External modems • CD/DVDs • Cameras and Scanners • MTPs • And the transfer of data to mobile devices	**Yes**	
	The proposed solution should feature cloud integration, to provide the fastest possible updates on malware and potential threats.	**Yes**	
	The proposed solution must have ability to manage user access rights for Read and Write operations on CDs/DVDs, removable storage devices and MTP devices.	**Yes**	
	The proposed solution must feature firewall filtering by local address, physical interface, and packet Time-To-Live (TTL).	**Yes**	
	The proposed solution must allow the administrator to monitor the application's use of custom/random ports after it has launched.	**Yes**	
	The proposed solution must support the blocking of prohibited (Deny-List) applications from being launched on the endpoint, and the blocking of all applications other than those included in Allow-Lists.	**Yes**	
	The proposed solution must have a cloud-integrated Application Control component for immediate access to the latest updates on application ratings and categories.	**Yes**	
	The proposed solution must offer protection to files executed in Windows Server containers.	**Yes**	
	The proposed solution must include traffic malware filtering, web link verification and web-resource control based on cloud categories.	**Yes**	
	The proposed solution Web Control/Restriction component must include a Cryptocurrencies and Mining category. It must also include predefined regional legal restrictions to comply with Belgian and Japanese Law.	**Yes**	
	The proposed solution must have the ability to allow applications based on their digital signature certificates, MD5, SHA256, META Data, File Path, and pre-defined security categories.	**Yes**	
	The proposed solution must have controls for the download of DLL and Drivers.	**Yes**	
	The proposed solution must support the control of scripts from PowerShell.	**Yes**	
	The proposed solution must support Test Mode with report generation on the launch of blocked applications.	**Yes**	
	The proposed solution must have the ability to restrict application activities within the system according to the trust level assigned to the application, and to limit the rights of applications to access certain resources, including system and user files "HIPS functionality".	**Yes**	
	The proposed solution must have the ability to control system/user application access to audio and video recording devices.	**Yes**	
	The proposed solution must provide a facility to check applications listed in each cloud-based category.	**Yes**	
	The proposed solution must have ability to integrate with a vendor-specific Advanced Threat Protection system.	**Yes**	
	The proposed solution must have ability to automatically regulate the activity of programs running, including access to the file system and registry as well as interaction with other programs.	**Yes**	
	The proposed solution must have the ability to automatically delete Application Control rules if an application is not launched during a specified interval. The interval must be configurable.	**Yes**	
	The proposed solution must have ability to automatically categorize applications launched prior to endpoint protection installation.	**Yes**	
	The proposed solution must have endpoint mail threat protection with: • Attachment filter and the ability to rename attachments. • Scanning of mail messages when receiving, reading and sending.	**Yes**	

	The proposed solution must have the ability to scan multiple redirects, shortened URLs, hijacked URLs, and time-based delays.	**Yes**	
	The proposed solution must enable the user of the computer to perform a check on a file's reputation from the File Context menu.	**Yes**	
	The proposed solution must include the scanning of all scripts, including those developed in Microsoft Internet Explorer, as well as any WSH scripts (JavaScript, Visual Basic Script WSH scripts (JavaScript, Visual Basic Script etc.), launched when the user works on the computer, including the internet.	**Yes**	
	The proposed solution must provide protection against as yet unknown malware based of the analysis of their behavior and examination of changes in the system register, together with a strong remediation engine to automatically restore any system changes made by the malware.	**Yes**	
	The proposed solution must provide protection against hacker attacks by using a firewall with an intrusion detection and prevention system (IDS/IPS) and network activity rules for more popular applications when working in computer networks of any type, including wireless networks.	**Yes**	
	The proposed solution must include IPv6 protocol support.	**Yes**	
	The proposed solution must offer scanning of critical sections of the computer as a standalone task.	**Yes**	
	The proposed solution must incorporate Application Self-Protection technology: • protecting against unauthorized the remote management of an application service. • protecting access to application parameters by setting a password. • preventing the disabling of protection by malware, criminals or amateur users.	**Yes**	
	The proposed solution must offer the ability to choose which threat protection components to install.	**Yes**	
	The proposed solution must include the antivirus checking and disinfection of files that have been packed using programs like PKLITE, LZEXE, DIET, EXEPACK, etc.	**Yes**	
	The proposed solution must include the anti-malware checking and disinfection of files in archives using the RAR, ARJ, ZIP, CAB, LHA, JAR, ICE formats, including password-protected files.	**Yes**	
	The proposed solution must protect against as yet unknown malware belonging to registered families, based on heuristic analysis.	**Yes**	
	The proposed solution must include multiple ways to notify the administrator about important events which have taken place (mail notification, audible announcement, pop-up window, log entry).	**Yes**	
	The proposed solution must allow the administrator to create a single installer with the required configuration, for use by non-IT literate users.	**Yes**	
2.	**Functional requirements: Detection**		
	The suggested solution must supplement verdict information from Endpoint Protection solution with system artefacts about the detection.	**Yes**	
	The suggested solution must support auto generation of threat indicators (IoC) after detection occurs with ability to apply response action.	**Yes**	
	The solution must have the capability to force run IoC scan across all endpoints with installed EP applications.	**Yes**	
	The suggested solution must support IoC scanning run according to a scheduler.	**Yes**	
	The suggested solution must support import of third-party IoC in OpenIoC format for its use in network scanning.	**Yes**	
	The suggested solution must support scanning using auto generated, uploaded or external (third-party) set of IoCs to detect earlier undetected threats.	**Yes**	
	The suggested solution must support exporting of IoC generated by the solution to a file in OpenIoC format.	**Yes**	
	Functional requirements: Visibility	**Yes**	
	The suggested solution must generate detailed alert card related to the detected threat on the endpoints.	**Yes**	
	An alert card must include at least the following information about detected threat: - Threat development chain graph (kill chain). - Information about the device on which the threat is detected (name, IP address, MAC address, user list, operating system).	**Yes**	

	- General information about the detection, including detection mode. - Registry changes associated with the detection. - History of the file presence on the device. Response actions performed by the application.		
	Threat development chain (kill chain) graph must provide visual information about the objects involved in the alert, for example, about key processes on the device, network connections, libraries, registry, etc.	**Yes**	
	An alert card must present detailed view on system artefacts and alert-related data for root cause analysis: - Process spawning - Network connections - Registry changes - Downloading object Dropped objects, etc.	**Yes**	
	Functional requirements: Response		
	The suggested solution must support ‘Single-click” response form management console	**Yes**	
	The suggested solution must support at least the following response actions that an administrator can perform when threats are detected:	**Yes**	
	Prevent object execution	**Yes**	
	o EDR solution must support both modes: records to the events about attempts to launch objects or open documents that meet the criteria of the Execution prevention, but does not block launch or opening these objects. blocks launch of the objects or opening the documents that meet criteria of the Execution prevention rules.	**Yes**	
	EDR solution must support blocking objects by hash (MD5 or SHA256) or by path pattern.	**Yes**	
	EDR solution must support blocking executables, scripts and documents	**Yes**	
	EDR solution must support notification user about prevention option	**Yes**	
	Host isolation.	**Yes**	
	EDR solution must provide means of isolating machine from the rest of the network in case of security incident, while preserving controlled communication with agents’ administration and management server.	**Yes**	
	EDR solution must support creating custom host isolation rules (i.e. adding particular network resources to exclusion e.g. DNS or selecting predefined profiles)	**Yes**	
	EDR solution must support manual bringing host back online from isolation.	**Yes**	
	Delete object from host or group of hosts.	**Yes**	
	Get (download) file from a host or group of hosts.	**Yes**	
	Terminate a process on the device.	**Yes**	
	Quarantine an object	**Yes**	
	The suggested solution must support object recovery from quarantine.	**Yes**	
	Run system scan	**Yes**	
	Remote program / process / command execution	**Yes**	
	Start IoC scan for a group of hosts.	**Yes**	
	The suggested solution must support ‘Single-click” response form management console	**Yes**	
Centralized administration, monitoring and update software requirements			
	The proposed solution must enable the installation of anti-malware software from a single distribution package.	**Yes**	Antivirus Licenses: Kaspersky Endpoint
	The proposed solution must have customizable installation profiles depending on the number of protected nodes.	**Yes**	

	The proposed solution must support IPv6 addresses.	**Yes**	Security for Business – Select/ Kaspersky Endpoint Detection and Response Optimum Add-on
	The proposed solution must support two-step verification (authentication).	**Yes**	
	The proposed solution must have ability to read information from Active Directory to obtain data about computer accounts in the organization.	**Yes**	
	The proposed solution must include a built-in web console for the management of the endpoints, which should not require any additional installation.	**Yes**	
	The proposed solution's web management console should be straightforward to use and must support touch screen devices.	**Yes**	
	The proposed solution must automatically distribute computer accounts by management group if new computers appear on the network. It must provide the ability to set the transfer rules according IP address, type of the operating system and location in Organizational Units of Active Directory.	**Yes**	
	The proposed solution must provide for the centralized installation, update and removal of anti-malware software, together with centralized configuration, administration, and the viewing of reports and statistical information about its operation.	**Yes**	
	The proposed solution must feature the centralized removal (manual and automatic) of incompatible applications from the administration center.	**Yes**	
	The proposed solution must provide flexible methods for anti-malware agent installation: RPC, GPO, an administration agent for remote installation and the option to create a standalone installation package for local installation.	**Yes**	
	The proposed solution must enable the remote installation of anti-malware software with the latest anti-malware databases.	**Yes**	
	The proposed solution must feature the automatic update of anti-malware software and anti-malware databases.	**Yes**	
	The proposed solution must have automatic search facilities for vulnerabilities in applications and in the operating system on protected machines.	**Yes**	
	The proposed solution must enable the management of a component prohibiting the installation and/or running of programs.	**Yes**	
	The proposed solution must enable the management of a component controlling work with external I/O devices.	**Yes**	
	The proposed solution must enable the management of a component controlling user activity on the internet.	**Yes**	
	The proposed solution must allow for the testing of downloaded updates by means of the centralized administration software prior to distributing them to client machines, and the delivery of updates to user workplaces immediately after receiving them.	**Yes**	
	The proposed solution must be able to automatically deploy protection to virtual infrastructures based on VMware ESXi, Microsoft Hyper-V, Citrix XenServer virtualization platform or hypervisor.	**Yes**	
	The proposed solution must enable the creation of a hierarchy of administration servers at an arbitrary level and the ability to centrally managing the entire hierarchy from the upper level.	**Yes**	
	The proposed solution must support Managed Services Mode for administration servers, so that logically isolated administration server instances can be set up for different users and user groups.	**Yes**	
	The proposed solution must give access to the anti-malware security vendor's cloud services via the administration server.	**Yes**	
	The proposed solution must include the automatic distribution of licenses on client computers.	**Yes**	
	The proposed solution must be able to perform inventories of software and hardware installed on user computers.	**Yes**	
	The proposed solution must have a notification mechanism to inform users about events in the installed anti-malware software and settings, and to distribute notifications about events via email.	**Yes**	
	The proposed solution must enable the centralized installation of third-party applications on all or selected computers.	**Yes**	
	The proposed solution must have the ability to specify any computer in the organization as a center for relaying updates and installation packages, in order to reduce the network load on the main administration server system.	**Yes**	

	The proposed solution must have the ability to specify any computer in the organization as a center for forwarding anti-malware agent events from the selected group of client computers to the centralized administration server, in order to reduce the network load on the main administration server system.	**Yes**	
	The proposed solution must be able to generate graphical reports for anti-malware software events, and data about the hardware and software inventory, licensing, etc.	**Yes**	
	The proposed solution must be able to export of reports to PDF and XML files.	**Yes**	
	The proposed solution must provide the centralized administration of backup storages and quarantine on all network resources where the anti-malware software is installed.	**Yes**	
	The proposed solution must provide the creation of internal accounts to authenticate administrators on the administration server.	**Yes**	
	The proposed solution must provide the creation of an administration system backup copy with the help of integrated administration system tools.	**Yes**	
	The proposed solution must support Windows Failover Cluster.	**Yes**	
	The proposed solution must have a built-in clustering feature.	**Yes**	
	The proposed solution must include some form of system to control virus epidemics.	**Yes**	
	The proposed solution must include Role Based Access Control (RBAC), and this must allow restrictions to be replicated throughout the management servers in the hierarchy.	**Yes**	
	The proposed solution's management server must include pre-defined security roles for the Auditor, Supervisor and Security Officer.	**Yes**	
	The proposed solution must have ability manage mobile devices through remote commands.	**Yes**	
	The proposed solution must have ability to delete downloaded updates.	**Yes**	
	The proposed solution must enable Administration Server updates to be managed from the application interface.	**Yes**	
	The proposed solution must provide the ability to select an update agent for client computers based on analysis of the network.	**Yes**	
	The proposed solution must clearly show information about the distribution of vulnerabilities across managed computers.	**Yes**	
	The proposed solution's management server interface must support the Arabic language.	**Yes**	
	The proposed solution's management server must maintain a revision history of the policies, tasks, packages, management groups created, so that modifications to a particular policy/task can be reviewed.	**Yes**	
	The proposed solution's management server must have functionality to create multiple profiles within a protection policy with different protection settings that can be simultaneously active on a single/multiple devices based on the following activation rules: • Device status • Tags • Active directory • Device owners • Hardware	**Yes**	
	The proposed solution must support following notification delivery channels: • Email • Syslog • SMS • SIEM	**Yes**	
	The proposed solution must have the ability to define an IP address range, in order to limit client traffic towards the management server based on time and speed.	**Yes**	
	The proposed solution must have the ability to perform inventory on scripts and .dll files.	**Yes**	
	The proposed solution must have the ability to tag/mark computers based on: • Network Attributes	**Yes**	

	o Name o Domain and/or Domain Suffix o IP address o IP address to management server • Location in Active Directory o Organizational Unit o Group • Operating System o Type and Version o Architecture o Service Pack number • Virtual Architecture • Application registry o Application name o Application version o Manufacturer		
	The proposed solution must have the ability to create/define settings based on a computer's location in the network, rather than the group to which it belongs in the management server.	**Yes**	
	The proposed solution must have the functionality to add a unidirectional connection mediator between the management server and the endpoint connecting over the internet/public network.	**Yes**	
	The proposed solution must allow the administrator to define restricted settings in policy/profile settings, so that a virus scan task can be triggered automatically when a certain number of viruses are detected over defined amount of time. The values for the number of viruses and timescale must be configurable.	**Yes**	
	The proposed solution must have a customizable dashboard generating and displaying real time statistics for endpoints.	**Yes**	
	The proposed solution must allow the administrator to customize reports.	**Yes**	
	The proposed solution must have the functionality to detect non-persistent virtual machines and automatically delete them and their related data from the management server when powered off.	**Yes**	
	The proposed solution must enable the administrator to set a period of time after which a computer not connected to the management server, and its related data are automatically deleted from the server.	**Yes**	
	The proposed solution must allow the administrator to create categories/groups of application based on: • Application Name • Application Path • Application Metadata • Application Digital certificate • Vendor pre-defined application categories • SHA • Reference computers to allow/deny their execution on endpoints.	**Yes**	
	The proposed solution must allow the administrator to define different status change conditions for groups of endpoints in the management server.	**Yes**	
	The proposed solution must allow the administrator to add custom/3rd party endpoint management tools into the management server.	**Yes**	
	The proposed solution must have a built-in feature/module to remotely collect the data needed for troubleshooting from the endpoints, without requiring physical access.	**Yes**	
	The proposed solution must allow the administrator to create a Connection Tunnel between a remote client device and the management server if the port used for connection to the management server is not available on the device.	**Yes**	
	Suggest solution must have built-in functionality to remotely connect to the endpoint using Windows Desktop Sharing Technology. In addition, the solution must be able to maintain the auditing of administrator actions during the session.	**Yes**	
	The proposed solution must have a feature to create a structure of administration groups using the Groups hierarchy, based on the following data: • structures of Windows domains and workgroups	**Yes**	

	• structures of Active Directory groups • contents of a text file created by the administrator manually		
	The proposed solution must be able to retrieve information about the equipment detected during a network poll. The resulting inventory should cover all equipment connected to the organization's network. Information about the equipment should update after each new network poll. The list of detected equipment should cover the following: • devices • mobile devices • network devices • virtual devices • OEM components • computer peripherals • connected devices • VoIP phones • network repositories The administrator must be able to add new devices to the equipment list manually or edit information about equipment that already exists on the network. 'Device is Written Off' functionality must be available, so that such devices are not displayed in the equipment list.	**Yes**	
	The proposed solution must incorporate a single distribution/relay agent to support at least 10,000 endpoints for the delivery of protection, updates, patches, and installation packages to remote sites.	**Yes**	
	The proposed solution must incorporate a single distribution/relay agent to relay/transfer or proxy threat reputation requests from endpoints to the management server.	**Yes**	
	The proposed solution must support the download of differential files rather than full update packages.	**Yes**	
	The proposed solution must support OPEN API, and include guidelines for integration with 3rd party external systems.	**Yes**	
	The proposed solution must include a built-in tool to perform remote diagnostics and collect troubleshooting logs without requiring physical access to the computer.	**Yes**	
	The proposed solution must include Role Based Access Control (RBAC) with customizable predefined roles.	**Yes**	
	The proposed solution's master/primary/parent management server must be able to relay updates and cloud reputation services.	**Yes**	
	The proposed solution's reports must include information about each threat and the technology that detected it.	**Yes**	
	The proposed solution report must include details about which endpoint protection components are, or are not, installed on client devices, regardless of the protection profile applied/existing for these devices.	**Yes**	
	The proposed solution's primary management server must be able to retrieve detailed information reporting on the health status etc. of managed endpoints from the secondary management servers.	**Yes**	
	The proposed solution must include the option for the customer to either deploy an on-premises management console, or use the vendor-provided cloud-based management console.	**Yes**	
	The proposed solution must be able to integrate with the vendor's cloud-based management console for endpoint management at no additional cost.	**Yes**	
	The proposed solution must enable swift migration from the on-premises management console to the vendor cloud-based management console.	**Yes**	
	The proposed solution must include support for cloud-based deployment via: • Amazon Web Services • Microsoft Azure	**Yes**	
	The proposed solution must provide anti-malware database update mechanisms including: • Multiple ways of updating, including global communication channels over the HTTPS protocol, shared resource at local network and removable media. • Verification of the integrity and authenticity of updates by means of an electronic digital signature.	**Yes**	
	The proposed solution must support Single Sign On (SSO) using NTLM and Kerberos.	**Yes**	

	Administration & Reporting EDR		
	The suggested solution must support secure communication between management console and endpoints with EDR agent	**Yes**	
	The suggested solution must support management of EDR agent through command line interface	**Yes**	
	Suggested solution must have inbuilt feature/module to collect the data required for troubleshooting, without require a physical access to the endpoint.	**Yes**	
	EDR application must have self-defence mechanism to prevent modifying its files/system components entries etc.	**Yes**	
	The solution must allow the creation of accounts with different roles used to administer the solution, just monitor the alerts, or review changes	**Yes**	
	The solution should be able to send email notifications when certain types of security alerts are generated.	**Yes**	
	Requirements for the solution documentation. A documentation for EDR software, including administration tools, should include at least online help for Administrators	**Yes**	
	Suport local de la Ofertant; Lucrările de instalare, configurare, punerea în funcțiune a soluției și asigurarea suportului la definirea/configurarea politicilor inițiale Training Beneficiarului - min. 3 persoane; Furnizarea documentației de instalare, (passport system și sistemul de administrare; Configurare, restabilire a serviciului oferit + Training + documentația, trebuie să fie executate de Ofertant, iar costul acestora trebuie să fie incluse în ofertă; Servicii de intervenție în mod continuu 24h/zi – 7zile/săptămână pentru alerte cibernetice ce conţin următoarele activităţi: - Efectuarea interogări de bază pentru a aduna informaţii suplimentare legate de incidentul de securitate - Echipa de support local se va conecta la consola de management a acestuia și va actualiza progresul / rezolvarea incidentelor de Securitate - Echipa de support local va investiga evenimentele de securitate și va escalada la nivelul 2 de intervenție - Echipa de support local va asigura gestionarea și prioritizarea alertelor, gestionarea răspunsurilor la incidente și escaladarea acestora - Echipa de support local va asista personalul superior al utilizatorilor finali în probleme de securitate, daca va fi necesar. - Echipa de support local va valida atacurile, evalua impactul, recomandă contramăsurile și va lucra în implementarea soluției de mitigare şi răspuns. - Echipa de support local va emite recomandări de ajustare a produsului/ tehnologiei de securitate către IS Posta Moldovei - Echipa de support local va colabora cu părţile interesate ale Clientului pentru a asigura rezolvarea în timp util a problemelor de securitate ridicate și critice - Echipa de support localva prioritiza și gestiona escaladarea incidentelor validate catre IS Posta Moldovei Autorizarea de la producător - Manufacture Authorization Letter.	**Yes**	

Anexa nr. 22
la Documentația standard
aprobată prin Ordinul Ministrului Finanţelor
nr. 115 din 15.09.2022

Specificații tehnice

Numărul procedurii de achiziție: *ocds-b3wdp1-MD-1691570951766 (21087716) din 09.08.2023.*	
Obiectul achiziției: Software Antivirus.	

Denumirea bunurilor/serviciilor	Denumirea modelului bunului/ serviciului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	**5**	6	7
Bunuri/servicii						
Software Antivirus	Kaspersky Endpoint Security for Business – Select 3 Y& Kaspersky Endpoint Detection and Response Optimum Add-on 3 Y	UE	Kaspersky	Conform Anexei nr.1	Conform Anexei nr.1	-
TOTAL						

Nume: Anatolie BULGARU
Poziția: Head of B2B IoT and ICT
Data: 28.08.2023
Locul: Chișinău Republica Moldova

Acest act este semnat prin aplicarea **Semnăturii Mobile**
Verificarea semnăturii - https://msign.gov.md/#/verify/upload

Anexa nr. 23
la Documentația standard
aprobată prin Ordinul Ministrului Finanţelor
nr. 115 din 15.09.2021

Specificații de preț

Numărul procedurii de achiziție: *ocds-b3wdp1-MD-1691570951766 (21087716) din 09.08.2023.*
Obiectul achiziției: Software Antivirus

Cod CPV	**Denumirea bunurilor/serviciilor**	**Unitatea de măsură**	**Cantitatea**	**Preț unitar (fără TVA)**	**Preț unitar (cu TVA)**	**Suma fără TVA**	**Suma cu TVA**	**Termenul de livrare/prestare**	**Clasificație bugetară (IBAN)**
1	**2**	**3**	**4**	5	6	7	8	**9**	**10**
	Bunuri/servicii								
72200000-7	Software Antivirus	un.	500	491.25	589.50	245,625.00	294,750.00	din data semnării contractului până la 31.12.2023	-
	TOTAL					**245,625.00**	**294,750.00**		

Nume: Anatolie BULGARU
Poziția: Head of B2B IoT and ICT
Data: 28.08.2023
Locul: Chișinău Republica Moldova

Acest act este semnat prin aplicarea **Semnăturii Mobile**
Verificarea semnăturii - https://msign.gov.md/#/verify/upload

AGENȚIA SERVICII PUBLICE

Departamentul înregistrare şi licenţiere a unităţilor de drept

EXTRAS

din Registrul de stat al persoanelor juridice

Nr. **526338** data **13.07.2023**

Denumirea completă: **Întreprinderea Mixtă "ORANGE MOLDOVA" S.A.**
Denumirea prescurtată: **Î.M. "ORANGE MOLDOVA" S.A.**
Forma juridică de organizare: **Societate pe acțiuni de tip închis,**
Numărul de identificare de stat şi codul fiscal (IDNO): **1003600106115**
Data înregistrării de stat: **18.03.1998**
Modul de constituire: **nou creată.**
Succesiunea în drept: Întreprinderea Mixtă "ORANGE MOLDOVA" S.A., IDNO 1003600106115 din 18.03.1998, este succesoarea tuturor drepturilor şi obligaţiunilor Societăţii cu Răspundere Limitată "SUN COMMUNICATIONS", (IDNO 1003600061928) ca urmare a reorganizării acesteia prin fuziune (absorbție) în conformitate cu Contractul de fuziune din 25.04.2023 şi Actul de transmitere (primire-predare) din 25.04.2023.
Sediul: **MD-2071, str. Alba-Iulia, 75, mun. Chișinău, Republica Moldova.** tel.

Obiectul principal de activitate:
1. Telecomunicații
2. Repararea aparatelor de radio şi televiziune

Capitalul social: **179499609** lei,

Administrator: **SURUGIU OLGA, IDNP 0981202021274, în funcție pînă la data de 31.03.2025**

Prezentul extras este eliberat în temeiul art.34 al Legii nr.220-XVI din 19 octombrie 2007 privind înregistrarea de stat a persoanelor juridice şi a întreprinzătorilor individuali şi confirmă datele din Registrul de stat la data de: **13.07.2023**.

Registrator în domeniul înregistrării de stat **Novac Stela**

INSTITUȚIA PUBLICĂ "AGENȚIA SERVICII PUBLICE"
IDNO 1002600024700
REPUBLICA MOLDOVA
CHIȘINĂU
158

EB 0435055

Date cu caracter personal

REPUBLICA MOLDOVA

CERTIFICAT DE ÎNREGISTRARE

ÎNTREPRINDEREA MIXTĂ "ORANGE MOLDOVA" S.A.

ESTE ÎNREGISTRATĂ LA CAMERA ÎNREGISTRĂRII DE STAT

Numărul de identificare de stat - codul fiscal

1003600106115

Data înregistrării **18.03.1998**

Data eliberării **24.04.2007**

Bolboceanu Adela, registrator de stat

Funcţia, numele, prenumele persoanei care a eliberat certificatul

A. Bolboceanu

semnătura

MINISTERUL DEZVOLTĂRII INFORMAŢIONALE AL REPUBLICII MOLDOVA
CAMERA ÎNREGISTRĂRII DE STAT
1004600077777
109

L.Ş.

MD 0067000

maib

Nr. C180/E01792
12 decembrie 2022

CERTIFICAT

Banca comercială „MAIB" S.A., confirmă că **I.M. ORANGE MOLDOVA S.A.**, IDNO **1003600106115** este deținător al următoarelor conturi bancare:

Cod IBAN	Valuta contului
MD64AG000000225110801767	MDL

Certificatul este eliberat la solicitarea titularului de cont, pentru a fi prezentat la cerere. Prezentul certificat este eliberat în scop informativ şi nu prezintă careva obligaţiuni financiare din partea Băncii.

Dumitru Baxan,
Vicepreședinte al Comitetului de Conducere
al BC"MAIB"S.A.

B.C. "MAIB" S.A. · Republica Moldova, mun. Chişinău
5
maib

Modificat

SERVICIUL FISCAL DE STAT
ГОСУДАРСТВЕННАЯ НАЛОГОВАЯ СЛУЖБА

Aprobat de către Inspectoratul Fiscal Principal de Stat
prin ordinul nr. 04 din 06.01.2004

CERTIFICAT

DE ÎNREGISTRARE A SUBIECTULUI IMPUNERII CU TVA

780044

SUBIECTUL IMPUNERII ÎNREGISTRAT Зарегистрированный субъект налогообложения	
Denumirea Наименование	ÎM "Orange Moldova" SA
Data înregistrării Дата регистрации	01.04.1998
Adresa juridică Юридический адрес	mun. Chişinău str. Alba Iulia, 75
Codul fiscal Фискальный код	1003600106115
Numărul de înregistrare ca subiect impozabil cu TVA Номер регистрации в качестве субъекта налогообложения НДС	780044

Tipul activităţii economice desfăşurate în conformitate cu clasificatorul activităţilor Тип осуществляемой деятельности согласно статистическому классификатору деятельности	6420

PRIMA PERIOADĂ FISCALĂ ПЕРВЫЙ НАЛОГОВЫЙ ПЕРИОД	
din от 01.04.1998	**pînă la** до 01.08.1998

PERIOADĂ FISCALĂ ULTERIOARĂ ПОСЛЕДУЮЩИЙ НАЛОГОВЫЙ ПЕРИОД	
din от	**pînă la** до

Şeful DAGU

L. Morari

INSPECTORATUL FISCAL PRINCIPAL DE STAT DE PE LÎNGĂ MINISTERUL FINANŢELOR AL REPUBLICII MOLDOVA

LOC PENTRU ŞTAMPILĂ
МЕСТО ДЛЯ ПЕЧАТИ

DATA ANULĂRII ÎNREGISTRĂRII ДАТА АННУЛИРОВАНИЯ РЕГИСТРАЦИИ	

LOC PENTRU ŞTAMPILĂ
МЕСТО ДЛЯ ПЕЧАТИ

Î.S. F.E.P. «Tipografia Centrală»

ORDIN DE PLATA 1148148 DATA EMITERII 24 august 2023 TIP DOC : 1

PLATITI: 5833-33 LEI Cinci Mii Opt Sute Treizeci şi Trei LEI şi 33 Ban

PLĂTITOR
(R) I.M. ORANGE MOLDOVA S.A.

CODUL IBAN MD64AG000000225110801767
CODUL FISCAL: 1003600106115

PRESTATORUL PLĂTITOR: BC'MAIB'S.A. suc.'Petru Movila'

BENEFICIAR
(R) Posta Moldovei IS

CODUL IBAN MD36ML000000000225183434
CODUL FISCAL: 1002600023242

PRESTATORUL BENEFICIAR:
BC'Moldindconbank'S.A.

DESTINAŢIA PLĂŢII:

Plata conform fact.nr Internal Note nr.16700 din 23.08.2023 din 23.08.23 (/P102/5833.33/ Pentru garantia pentru oferta la procedura de achizitie prin LD)

TIPUL TRANSFERULUI NORMAL/URGENT

N

COD TRANZACŢIE:	DATA PRIMIRII:	DATA EXECUTĂRII:
001	24 august 2023 12:27:00	24 august 2023 12:29:00

Ora Primirii 1 2 : 2 7

SEMNĂTURA PRESTATORULUI

L.Ş.

Alexandru Simonov

Maria Rotaru

SEMNĂTURILE EMITENTULUI

L.Ş. internet-banking

BC„MAIB"S.A.
IDNO 1002600003778
25. AUG. 2023
12
Sucursala „Petru Movilă"
Republica Moldova, mun. Chişinău

MOTIVUL REFUZULUI:

“Orange Moldova” S.A.

Anexa nr.3
DECLARAȚIE
pe proprie răspundere privind îndeplinirea criteriilor de calificare și selecție

Titlul achiziției: Software Antivirus
Subsemnatul, Anatolie Bulgaru, reprezentantul legal al “Orange Moldova” S.A. în calitate de ofertant, la achiziție „Software Antivirus”, nr. ocds-b3wdp1-MD-1691570951766, organizată de *Î.S.”Poşta Moldovei”*, declar pe propria răspundere, sub sancțiunea excluderii din procedura de achiziție și a sancțiunilor aplicate faptei de fals în acte publice, că nu ne aflăm în situațiile prevăzute la:

- art. 70 al Legii nr. 74/2020:

a) nu se află în niciuna dintre situațiile de excludere menționate la art. 67 și 68;
b) îndeplinește criteriile privind capacitatea astfel cum a fost solicitat de entitatea contractantă;
c) dacă este cazul, îndeplinește criteriile de selecție stabilite de entitatea contractantă în conformitate cu prevederile Legii 74/2020.

- art. 67 al Legii nr. 74/2020, alin. 3).
- în ultimii 5 ani, a fost condamnat, prin hotărâre definitivă a unei instanțe judecătorești, pentru participare la activități ale unei organizații sau grupări criminale, pentru corupție, pentru fraudă și/sau pentru spălare de bani, pentru infracțiuni de terorism sau infracțiuni legate de activități teroriste, pentru finanțarea terorismului, exploatarea prin muncă a copiilor și pentru alte forme de trafic de persoane.
- art. 68 din Legea nr. 74/2020, ofertantul declară că nu se află în oricare dintre următoarele situații prevăzute de art. 19 Legea 131/2015 și anume:

a) se află în proces de insolvabilitate ca urmare a hotărîrii judecătoreşti;
b) nu şi-a îndeplinit obligaţiile de plată a impozitelor, taxelor şi contribuţiilor de asigurări sociale în conformitate cu prevederile legale în vigoare în Republica Moldova sau în ţara în care este stabilit;
c) a fost condamnat, în ultimii 3 ani, prin hotărîrea definitivă a unei instanţe judecătoreşti, pentru o faptă care a adus atingere eticii profesionale sau pentru comiterea unei greşeli în materie profesională;
d) a prezentat informaţii false sau nu a prezentat informaţiile solicitate de către autoritatea contractantă în scopul demonstrării îndeplinirii criteriilor de calificare şi selecţie;
e) a încălcat obligațiile aplicabile în domeniul mediului, muncii și asigurărilor sociale, în cazul în care autoritatea contractantă demonstrează, prin orice mijloace adecvate, acest fapt;
f) se face vinovat de o abatere profesională, care îi pune la îndoială integritatea, în cazul în care autoritatea contractantă demonstrează, prin orice mijloace adecvate, acest fapt;
g) a încheiat cu alți operatori economici acorduri care vizează denaturarea concurenței, în cazul în care acest fapt se constată prin decizie a organului abilitat în acest sens;
h) se află într-o situație de conflict de interese care nu poate fi remediată în mod efectiv prin măsurile prevăzute la art. 79.
i) este inclus în Lista de interdicţie a operatorilor economici;
j) nu respectă regimul de incompatibilități prevăzut la art. 16 alin. (6).

- art. 16 legea 131/2015:

persoanele fizice și juridice care sunt înregistrate, au reședința sau desfășoară activitatea economică principală în jurisdicții ori regiuni autonome ce nu implementează standarde internaționale de transparență, precum și persoanele juridice în componența cărora figurează, direct sau indirect, una sau mai multe persoane (fondatori, asociați, acționari, administratori, beneficiari efectivi) care sunt înregistrate, au reședința sau desfășoară activitatea economică principală în astfel de jurisdicții ori regiuni autonome. Metodologia de stabilire a jurisdicțiilor care nu implementează standarde internaționale de transparență, precum și lista jurisdicțiilor respective, în sensul prezentei legi, se aprobă de către Guvern, la propunerea Serviciului Prevenirea și Combaterea Spălării Banilor, după consultarea Băncii Naționale a Moldovei și a Comisiei Naționale a Pieței Financiare.

Data completării 28.08.2023

Cu stimă,
Anatolie Bulgaru
Head of B2B IoT and ICT
Î.M. „Orange Moldova” S.A.

Anexa nr. 12
la Documentația standard
aprobată prin Ordinul Ministrului Finanţelor
nr. 115 din 15.09.2021

DECLARAȚIE
privind lista principalelor livrari/prestări efectuate în ultimii 3 ani de activitate

Nr d/o	Obiectul contractului	Denumirea/numele beneficiarului/ Adresa	Calitatea Furnizorului /Prestatorului*)	Preţul contractului/ valoarea bunurilor/serviciilor livrate/prestate	Perioada de livrare/prestare (luni)
1	Soluţie Antivirus	Tirex Moldova	contractant unic	3,150.00 EUR inclusiv TVA.	Livrare unica anul 2021
2	Soluţie Antivirus	SUDZUCKER-MOLDOVA S.R..L.	contractant unic	1,700.00 EUR inclusiv TVA.	Livrare unica anul 2021
3	Soluţie Antivirus	Lukoil Moldova	contractant unic	380,000.00 MDL inclusiv TVA.	Livrare unica anul 2022
4	Echipament IT/Retea IP/Securitate Inf.	B.C. Victoriabank S.A.	contractant unic	360,000.00 USD inclusiv TVA.	Livrare unica anul 2021
5	Echipament IT/Retea IP/Securitate Inf.	BC ”MAIB” S.A.	contractant unic	130,000.00 EUR inclusiv TVA.	Livrare unica anul 2022
6	Echipament IT/Retea IP/Securitate Inf.	Noction S.R.L.	contractant unic	20,000.00 USD inclusiv TVA	Livrare unica anul 2022
7	Echipament IT/Retea IP/Securitate Inf.	IP STISC	contractant unic	5,745,000.00 MDL inclusiv TVA	Livrare unica anul 2022
8	Echipament IT/Retea IP/Securitate Inf.	IT-Lab Grup SRL	contractant unic	6,300.00 EUR inclusiv TVA.	Livrare unica anul 2022
9	Echipament IT/Retea IP/Securitate Inf.	Health Forever International SRL	contractant unic	27,000.00 EUR inclusiv TVA	Livrare unica anul 2023
10	Echipament IT/Retea IP/Securitate Inf.	ICT Solutii SRL	contractant unic	300,000.00 EUR inclusiv TVA.	Livrare unica anul 2023

Data completării 28.08.2023
Cu stimă,
Anatolie Bulgaru
Head of B2B IoT and ICT
Î.M. „Orange Moldova” S.A.

Acest act este semnat prin aplicarea Semnăturii Mobile
Verificarea semnăturii - https://msign.gov.md/#/verify/upload

DECLARAŢIE
privind termenul de plată a licenţelor

Către: **Întreprinderea de Stat POŞTA MOLDOVEI,**
mun. Chişinău, bd. Ștefan Cel Mare și Sfânt, nr. 134, MD-2012

Prin prezenta declarație, compania Î.M. Orange Moldova S.A., declară că în cadrul procedurii de achiziție publică de tip „Licitație deschisă" nr. **ocds-b3wdp1-MD-1691570951766** din data de 09.08.2023, achitarea pentru „**Software Antivirus"** va fi efectuata în termen de 30 zile (**treizeci zile**) din data recepţionării.

Data completării 28.08.2023

Cu stimă,
Anatolie Bulgaru
Head of B2B IoT and ICT
Î.M. „Orange Moldova" S.A.

Acest act este semnat prin aplicarea Semnăturii Mobile
Verificarea semnăturii - https://msign.gov.md/#/verify/upload

ECSI European Cyber Security Initiative

THE FOLLOWING DOCUMENT IS ISSUED AS A

CERTIFICATE

ON THE COMPLETION OF THE
COMPUTER SECURITY INCIDENT RESPONSE TEAM TRAINING

TO

Andrei Lunga

CHISINAU, REPUBLIC OF MOLDOVA

21 OCTOBER 2016

LAURI ALMANN
DIRECTOR

NATO
OTAN

This activity is supported by: The NATO Science for Peace and Security Programme

Kaspersky Certification

kaspersky

Certified
Professional

Kaspersky hereby confirms that

Andrei Lunga

has successfully completed all the requirements
to acquire the certificate:

Certified Professional: Kaspersky Endpoint Security and Management (002.11.6)

Issued on: **28 October 2021**
Certificate number: **002.11.6-AAS-0418035**

Eugene Kaspersky,
Chief Executive Officer

Kaspersky Certification

kaspersky

Certified
Professional

Kaspersky hereby confirms that

Ion Cozma

has successfully completed all the requirements
to acquire the certificate:

Certified Professional: Kaspersky Endpoint Security and Management (002.11.1)

Issued on: **15 December 2020**
Certificate number: **002.11.1-AAS-0088955**

Eugene Kaspersky,
Chief Executive Officer

kaspersky

kaspersky.com

Kaspersky Certification

kaspersky

Certified Professional

Kaspersky hereby confirms that

Mircea Grosu

has successfully completed all the requirements
to acquire the certificate:

Certified Professional: Kaspersky Endpoint Security and Management (002.11.6)

Issued on: **03 November 2021**
Certificate number: **002.11.6-AAS-0417742**

Eugene Kaspersky,
Chief Executive Officer

Kaspersky Certification

kaspersky

Certified Professional

Kaspersky hereby confirms that

Vitali Civga

has successfully completed all the requirements
to acquire the certificate:

Certified Professional: Kaspersky Endpoint Security and Management (002.11.1)

Issued on: **15 December 2020**
Certificate number: **002.11.1-AAS-0095747**

Eugene Kaspersky,
Chief Executive Officer

Kaspersky Certification

kaspersky

Accomplishment
Sales

Kaspersky hereby confirms that

Ion Ciorici

has successfully completed all the requirements
to acquire the certificate:

Accomplishment Sales: Kaspersky Small Office Security

Issued on: **13 December 2022**
Certificate number: **KSOS-AAS-0476711**

Eugene Kaspersky,
Chief Executive Officer

kaspersky

kaspersky.com

Kaspersky Certification

kaspersky

Sales
Specialist

Kaspersky hereby confirms that

Ion Ciorici

has successfully completed all the requirements
to acquire the certificate:

Sales Specialist: Kaspersky Endpoint Security Cloud (S40.16)

Issued on: **13 December 2022**
Certificate number: **S40.16-AAS-0476719**

Eugene Kaspersky,
Chief Executive Officer

Kaspersky Certification

kaspersky

Sales
Specialist

Kaspersky hereby confirms that

Ion Ciorici

has successfully completed all the requirements
to acquire the certificate:

Sales Specialist: Kaspersky Endpoint Security Cloud (S40.16)

Issued on: **13.12.2022**
Certificate #: **S40.16-AAS-0476719**

Eugene Kaspersky,
Chief Executive Officer

Kaspersky Certification

Kaspersky Partner
Onboarding Program
Accomplishment

Kaspersky hereby confirms that

Ion Ciorici

has successfully completed all the requirements to acquire the certificate:

Accomplishment: Partner Onboarding Program

Issued on: **14.12.2022**
Certificate #: **ONB001-AAS-0476725**

Eugene Kaspersky,
Chief Executive Officer

kaspersky

kaspersky.com

Kaspersky Certification

kaspersky

Sales
Specialist

Kaspersky hereby confirms that

Ion Ciorici

has successfully completed all the requirements
to acquire the certificate:

Sales Specialist: Kaspersky Endpoint Security for Business (S02.11.1)

Issued on: **14.12.2022**
Certificate #: **S02.11.1-AAS-0476769**

Eugene Kaspersky,
Chief Executive Officer

kaspersky

kaspersky.com

Kaspersky Certification

kaspersky

Sales
Specialist

Kaspersky hereby confirms that

Ion Ciorici

has successfully completed all the requirements
to acquire the certificate:

Sales Specialist: Kaspersky Security Foundations (S53.10)

Issued on: **15.12.2022**
Certificate #: **S53.10-AAS-0476947**

Eugene Kaspersky,
Chief Executive Officer

kaspersky

kaspersky.com

Kaspersky Certification

kaspersky

Sales
Specialist

Kaspersky hereby confirms that

Ion Ciorici

has successfully completed all the requirements
to acquire the certificate:

Sales Specialist: Kaspersky Optimum Security (S54.10)

Issued on: **16.12.2022**
Certificate #: **S54.10-AAS-0477064**

Eugene Kaspersky,
Chief Executive Officer

kaspersky

kaspersky.com

Kaspersky Certification

kaspersky

Sales Specialist

Kaspersky hereby confirms that

Ion Ciorici

has successfully completed all the requirements
to acquire the certificate:

Sales Specialist: Kaspersky Expert Security (S55.10)

Issued on: **20.12.2022**
Certificate #: **S55.10-AAS-0477193**

Eugene Kaspersky,
Chief Executive Officer

kaspersky

kaspersky.com

Kaspersky Certification

kaspersky

Certified
Professional

Kaspersky hereby confirms that

Ion Ciorici

has successfully completed all the requirements
to acquire the certificate:

Certified Professional: Kaspersky Endpoint Security Cloud (040.16)

Issued on: **26.12.2022**
Certificate #: **040.16-AAS-0477858**

Eugene Kaspersky,
Chief Executive Officer

kaspersky

kaspersky.com

Kaspersky Certification

kaspersky

Certified Professional

Kaspersky hereby confirms that

Ion Ciorici

has successfully completed all the requirements
to acquire the certificate:

Certified Professional: Kaspersky Endpoint Security and Management (002.11.6)

Issued on: **09.01.2023**
Certificate #: **002.11.6-AAS-0477351**

Eugene Kaspersky,
Chief Executive Officer

kaspersky

kaspersky.com

Kaspersky Certification

kaspersky

Certified
Professional

Kaspersky hereby confirms that

Ion Ciorici

has successfully completed all the requirements to acquire the certificate:

Certified Professional: Kaspersky EDR Optimum Presales (P24.2)

Issued on: **12.01.2023**
Certificate #: **P24.2-AAS-0477856**

Eugene Kaspersky,
Chief Executive Officer

kaspersky

kaspersky.com

Kaspersky
United

Partner Program

kaspersky

Silver Partner

Kaspersky hereby certifies that

Orange Moldova SA

Moldova

Silver Partner

is authorised to resell Kaspersky products and services.
The Kaspersky Partner agreement recognises the commitment of both companies to offer superior solutions and customer service

Certificate is valid till **31/01/2024**
Partner PIN **RA02MD00**

Andrey Efremov,
Chief Business Development Officer

Kaspersky Certification

kaspersky

Certified Professional

Kaspersky hereby confirms that

Andrei Lunga

has successfully completed all the requirements
to acquire the certificate:

Certified Professional: Kaspersky Endpoint Security and Management (002.11.6)

Issued on: **28 October 2021**
Certificate number: **002.11.6-AAS-0418035**

Eugene Kaspersky,
Chief Executive Officer

kaspersky

kaspersky.com

Kaspersky Certification

kaspersky

Sales
Specialist

Kaspersky hereby confirms that

Andrei Lunga

has successfully completed all the requirements
to acquire the certificate:

Sales Specialist: Kaspersky Endpoint Security for Business (S02.11.1)

Issued on: **13 October 2021**
Certificate number: **S02.11.1-AAS-0417934**

Eugene Kaspersky,
Chief Executive Officer

kaspersky

International cooperation, transparency, trust, risk management, and local responsibility: Five important pillars of Kaspersky's DNA

Kaspersky Romania is part of the global Kaspersky group, a privately held group of companies. The group's holding company is Kaspersky Labs Limited (KLL). It is registered in London, the UK. Kaspersky Romania is a 100% subsidiary of KLL. There are 13 legally independent Kaspersky national companies operating in various countries of Europe. These companies are all subsidiaries of KLL. Kaspersky Romania pays its taxes, salaries and social security contributions in Romania. The company also conducts research and development in Europe. Its Global Research and Analysis Team (GReAT) is managed from Bucharest.

This paper provides information on the following:

- How Kaspersky increases user protection and security through national as well as cross-border and cross-industry collaboration;
- Why strengthening cybersecurity and increasing cyber resilience drives our actions;
- Why Kaspersky considers transparency and trust to be the essential foundations for secure digitization.

Kaspersky's work is driven and motivated by the need of citizens, businesses, and governments in Europe and around the world to take advantage of the opportunities of digitalization in a secure, reliable, and trustworthy manner.

1/ Resilient, secure, transparent business processes

Kaspersky's business processes are designed for **maximum resilience**, so that customers and partners can rely on the **best possible business continuity** even in times of geopolitical tension. This is made possible by a balanced and structured distribution of tasks and responsibilities between HQ and the national subsidiaries, by **organizational**, **infrastructural** and **technical measures**, as well as comprehensive and goal-orientated **employee qualifications**. This enables us to ensure that we meet our obligations to partners, customers and potential new customers in the best possible way - from supplying products and providing support to securing financial transactions.

2/ Cooperation at European level

The European single market is the largest cybersecurity market in the world. This is also true for Kaspersky: Europe is the largest market for the company - across all industries. Therefore, Europe is central to Kaspersky's corporate strategy. Here, we collaborate with numerous national and international organizations. For example, we are involved in several studies and publications of the **European Union Agency for Cybersecurity, ENISA**. A researcher from our GReAT team is a member of the ENISA ad hoc working group on "EU Cyber Threat Landscapes." Together with Europol, the Dutch police, and McAfee, we also launched the **NoMoreRansom** global initiative. We are currently a consortium partner in four **European Horizon 2020** projects. Together with ENISA and the German Federal Office for Information Security (BSI), our experts contributed to a consultation on AI and cybersecurity of the European Parliament's AIDA Committee in January 2021.

3/ Global cooperation

Kaspersky is an industry partner of the **Council of Europe** to promote an open and secure internet, and is a partner of the **Geneva Dialogue on Responsible Behavior in Cyberspace**. Kaspersky has contributed to the **OECD 2021 reports** on digital security and vulnerability management, is one of the first signatories of the Paris Call for Trust & Security in Cyberspace, and participates in **United Nations discussion forums** such as the **UN Open Working Group on Information and Communication Technology Developments in the Context of International Security**, and contributes to the **Internet Governance Forum (IGF)**. We are involved in all these bodies and organizations because trustworthy cooperation and information sharing are essential in cybersecurity. Kaspersky is valued as a trusted partner in Europe and worldwide.

4/ Diversified financial system

Kaspersky has operated a diversified financial system since 2008. The national companies manage their finances independently – from the independent handling of income and expenses to the handling of partner orders. The country units conduct their financial transactions in their respective countries and use local banks.

5/ Global Transparency Initiative (GTI)

As part of the Global Transparency Initiative (GTI), Kaspersky has taken the following measures:

- Data storage and processing are located in Switzerland. Kaspersky operates a data infrastructure in two highly secure data centers in Zurich to process and store cyberthreat data from customers in Europe, the United States, and Canada, as well as several Asia-Pacific countries.
- Establishing "transparency centers" for reviewing source code, all versions of our builds and AV database, software development, and data management – including reviewing the information Kaspersky products send to the cloud-based Kaspersky Security Network (KSN). Kaspersky also provides access to its source code to ensure it matches publicly available modules. Kaspersky also provides the software bills of materials (SBOM) for its products. The transparency centers are located in Zurich, Madrid, Kuala Lumpur, and São Paulo.
- The security and reliability of our technical and organizational procedures and data services have been confirmed by two external, independent audit organizations. Kaspersky successfully passed in 2019 and again in 2022 the SOC-2 (Service Organization Control for Service Organizations) Type 1 audit by a Big Four auditor, which confirmed the security of Kaspersky's process for developing and releasing AV updates against the risk of unauthorized changes. In addition, our data services were certified according to ISO/IEC 27001:2013.
- Organizing our Vulnerability Management Program. In March 2018, as part of our bug bounty program, Kaspersky increased the bounties for external researchers who find critical vulnerabilities in the company’s products up to $100,000. Since then, Kaspersky has awarded 53 bounties even though no critical vulnerability has ever been reported. With this approach to vulnerability analysis, management and disclosure, Kaspersky is constantly improving the security of its products. To create more transparency in vulnerability management, Kaspersky has published ethical principles for responsible vulnerability disclosure.

Nr: 230820231
Customer: ÎS Posta Moldovei
Contest: ID ocds-b3wdp1-MD-1691570951766
Procurement subject: Software Antivirus

Manufacturer's Authorization Form

By this letter, **KASPERSKY INFO SYSTEMS SRL** who is established and reputable manufacturer of Kaspersky Anti Virus having its registered office at Dimitrie Pompei 9-9A, Iride Business Park, Building 24, 1st floor, District 2, Bucharest, Romania officially confirms that **Orange Moldova SA (Partner PIN RA02MD00), str. Alba Iulia 75, Chisinau, Republic of Moldova,** is an authorized partner of Kaspersky and is entitled to supply, install, offer technical support 24x7, trainings and maintain Kaspersky solutions in Republic of Moldova.

Kaspersky Lab confirm technical support 24x7 offered also in Ro Language.

Territory Channel Manager

Kaspersky Lab **Bogdan Albu**

Date: August 22, 2023

SOCIETATEA COMERCIALA
KASPERSKY INFO SYSTEMS S.R.L.
BUC
ROMANIA