Phần 2. YÊU CẦU VỀ KỸ THUẬT

Chương V. YÊU CẦU VỀ KỸ THUẬT

Mục 1. Yêu cầu về kỹ thuật

Yêu cầu về kỹ thuật bao gồm các nội dung cơ bản như sau:

1.1. Giới thiệu chung về dự án/dự toán mua sắm, gói thầu

- Chủ đầu tư: Trung tâm Công nghệ thông tin, Bộ Nội vụ

- Địa chỉ: Số 8 Tôn Thất Thuyết, Cầu Giấy, Hà Nội

- Dự toán mua sắm: Thực hiện Quyết định số 88/QĐ-CNTT ngày 06/11/2025 của Giám đốc Trung tâm Công nghệ thông tin về việc phê duyệt điều chỉnh Kế hoạch lựa chọn nhà thầu Mua sắm tài sản và thuê dịch vụ năm 2025 của Trung tâm Công nghệ thông tin.

- Tên gói thầu: Mua bản quyền phần mềm tại Trung tâm tích hợp dữ liệu Bộ Nội vụ.

- Công việc chính của gói thầu:

Phần 1: Mua 01 năm bản quyền phần mềm diệt Virus cho máy chủ, máy trạm, phòng chống Virus mạng của hãng của hãng Kaspersky Next EDR Foundation: Mua bản quyền phần mềm diệt Virus cho các máy chủ, máy trạm của hãng của hãng Kaspersky Next EDR Foundations (650 node) tại trụ sở chính của Bộ số 8 Tôn Thất Thuyết và Trung tâm Tích hợp dữ liệu số 12 Ngô Quyền.

Phần 2: Mua 01 năm bản quyền cập nhật phần mềm Mail-SeCure cho hệ thống thư điện tử công vụ:Mua 01 năm bản quyền cập nhật phần mềm Mail-SeCure cho hệ thống thư điện tử công vụ của Bộ Nội vụ.

- Thời gian thực hiện gói thầu:

Phần 1: Mua 01 năm bản quyền phần mềm diệt Virus cho máy chủ, máy trạm, phòng chống Virus mạng của hãng của hãng Kaspersky Next EDR Foundation:

+ Thời gian bàn giao giấy chứng nhận bản quyền các phần mềm là 30 ngày kể từ ngày Hợp đồng có hiệu lực.

+ Thời gian bản quyền là 01 năm kể từ ngày bản quyền được kích hoạt.

Phần 2: Mua 01 năm bản quyền cập nhật phần mềm Mail-SeCure cho hệ thống thư điện tử công vụ:

+ Thời gian bàn giao giấy chứng nhận bản quyền các phần mềm là 30 ngày kể từ ngày Hợp đồng có hiệu lực.

+ Thời gian gia hạn bản quyền là 01 năm kể từ ngày bản quyền được kích hoạt.

1.2. Yêu cầu về kỹ thuật

Thông số kỹ thuật của hàng hóa và các dịch vụ liên quan phải tuân thủ các thông số kỹ thuật và các tiêu chuẩn sau đây:

Phần 1: Mua 01 năm bản quyền phần mềm diệt Virus cho máy chủ, máy trạm, phòng chống Virus mạng của hãng Kaspersky Next EDR Foundation

Hạng mục số	Tên hàng hóa/dịch vụ liên quan	Thông số kỹ thuật và các tiêu chuẩn	Yêu cầu khác
1	**Phần mềm diệt virus cho máy Chủ, máy Trạm**	**Hỗ trợ triển khai các hệ điều hành:** - Hệ điều hành Microsoft 7sp1, 8, 10,11 - Hệ điều hành Microsoft Windows Server 2008 sp1, 2012, 2016, 2019, 2022, 2025 - Có bộ cài bảo vệ cho các hệ điều hành Mobile: iOS, Android - Hỗ trợ hệ điều hành Linux: Red Hat, CentOS, SuSe, Ubuntu, Debian, AlmaLinux OS, AlterOS, Amazon, Astra, EMIAS, EulerOS, Oracle, Goslinux… - Hỗ trợ hệ điều hành MAC từ phiên bản MAC OS 12-15	
		Chức năng Anti-Virus: - Có khả năng phát hiện và diệt viruses, spyware, worm, trojan rootkit, Keyloger Macro,… - Cho phép lựa chọn quét nhanh, quét full, quét tức thời, quét theo lịch trình và hỗ trợ quét từ xa qua giao diện quản lý tập trung. - Giải pháp hỗ trợ quét thời gian thực các file truy xuất. - Có khả năng chỉ quét những file mới và những file có sự thay đổi so với lần quét virus gần nhất giúp tăng tốc độ quét virus	

Hạng mục số	Tên hàng hóa/dịch vụ liên quan	Thông số kỹ thuật và các tiêu chuẩn	Yêu cầu khác
		- Giải pháp phải quét bộ nhớ hệ thống để phái hiện các rootkit, tiến trình ẩn, và các hành vi khác cho thấy mã độc hại đang cố gắng ẩn giấu. - Giải pháp có chức năng bảo vệ Web , đáp ứng quét cho traffic web, email, file theo cơ chế chủ động. - Giải pháp đáp ứng chức năng thông báo cho người sử dụng và quản trị hệ thống về việc phát hiện đối tượng bị nhiễm mã độc qua hộp thoại cảnh báo cho người sử dụng; Email, SMS và gửi tới SIEM cho người quản trị. - Cho phép người quản trị có thể thiết lập mặc định các hành động sẽ thực hiện khi chương trình phát hiện mã độc: Alert/Notify, Clean, Delete/Remove, Move/ Quarantine. - Hỗ trợ các tính năng mà nhờ đó người quản trị có thể lập kế hoạch ngăn chặn việc bùng nổ lây lan virus trong hệ thống. - Giải pháp có chức năng Quanrantine đối tượng bị nghi lây nhiễm trước khi thực hiện Repair/Delete, khi cần có thể Restore lại từ các file này. - Bảo vệ các nguy cơ từ Email bằng việc quét toàn bộ các Email vào/ra để phát hiện và ngăn chặn các nguy cơ từ Email. Hỗ trợ các giao thức: POP3, SMTP, IMAP	
		Chức năng HIPS (Host IPS): Ngăn chặn xâm nhập vào máy chủ ngăn chặn các ứng dụng thực hiện các hành vi nguy hiểm cho hệ điều hành đảm bảo quyền truy vào tài nguyên hệ điều hành và dữ liệu cá nhân	
		Chức năng giám sát mạng và giám sát hệ thống: - Cho phép xem toàn bộ các kết nối mạng trên máy tính theo thời gian thực.	

Hạng mục số	Tên hàng hóa/dịch vụ liên quan	Thông số kỹ thuật và các tiêu chuẩn	Yêu cầu khác
		- Cho phép ghi lại hoạt động của các ứng dụng trên máy tính, cung cấp thông tin này để nâng cao tính bảo mật.	
		Chức năng Firewall: - Phải có chức năng hỗ trợ kiểm soát traffic vào/ra. - Cho phép thao tác kiểm soát Firewall Client từ xa như: Disable, Enable từ xa. - Giải pháp phải có khả năng cảnh báo, giám sát các ứng dụng đang chạy. - Cho phép tạo ra tập luật (rule) dựa trên ứng dụng hoặc mạng (application network, network packet rule). Hỗ trợ các dạng protocol: TCP, UDP, ICMP, ICMPv6, IGMP, và GRE.	
		Chức năng Device control: - Phải có khả năng ngăn chặn thiết bị nào có thể hoặc không thể sử dụng trên Windows. - Phải có khả năng ngăn cấm các ứng dụng chạy từ thiết bị lưu trữ ngoài. - Phải có khả năng thiết lập lịch được sử dụng thiết bị cắm ngoài qua giao tiếp USB. - Cho phép thiết lập danh sách các thiết bị cắm ngoài được sử dụng (Trusted Device).	
		Chức năng Web Control: - Lọc Web theo URL, Category, Data, Content. - Giới hạn truy cập Web theo lịch - Cho phép quét toàn bộ giao tiếp thông qua giao thức HTTP, HTTPS, kiểm tra toàn bộ URL xem có trong danh sách các website chứa mã độc hay website lừa	

Hạng mục số	Tên hàng hóa/dịch vụ liên quan	Thông số kỹ thuật và các tiêu chuẩn	Yêu cầu khác
		đảo hay không. - Cho phép tạo ra các luật để hạn chế hay cấm người dùng truy cập vào những nội dung không Cho phép. - Tập luật có thể thực hiện theo lịch, Cho phép các luật thực hiện theo thời gian cụ thể.	
		Chức năng Application Control: - Cho phép thiết lập danh sách trắng bằng việc phân loại các ứng dụng theo đánh giá của nhà sản xuất, hoặc sử dụng công nghệ điện toán đám mây. - Cho phép tạo ra danh sách trắng các ứng dụng theo nhóm người sử dụng bằng việc kết hợp với AD/LDAP. - Khả năng thiết lập danh sách đen các ứng dụng theo nhóm, theo sự phân loại của nhà sản xuất hoặc theo cơ chế bảo mật của mỗi đơn vị sử dụng.	
		Chức năng Virus Update: - Hỗ trợ update bằng tay tại Client từ Server quản lý. - Hỗ trợ Update cho nhiều Client từ Server quản lý. - Hỗ trợ lập lịch tự động download update. - Server quản lý trung gian: Có thể tải Update từ nhiều nguồn khác nhau (từ server quản lý cấp trên, từ nhà cung cấp qua Internet), có thể thiết lập việc lựa chọn nguồn update. - Giao thức dùng để update virus từ nhà cung cấp, từ máy chủ là giao thức chuẩn: HTTP, HTTPS, FTP, SMB share và có thể hoạt động thông qua Proxy.	
		Chức năng quét lỗ hổng bảo mật: - Có khả năng quét lỗ hổng bảo mật các sản phẩm của Microsoft và các hãng	

Hạng mục số	Tên hàng hóa/dịch vụ liên quan	Thông số kỹ thuật và các tiêu chuẩn	Yêu cầu khác
		khác. - Bảo vệ thiết bị khỏi ransomware bao gồm cả các thư mục chia sẻ trên máy chủ (ransomware including protection for server share folders) - Phục hồi dữ liệu bị nhiễm mã độc (Malicious action rollback)	
		Một số chức năng bảo vệ khác: Thành phần bảo vệ AMSI hỗ trợ quét phần mềm độc hại từ Microsoft Khả năng tự bảo vệ: - Phần mềm diệt virus phải có khả năng tự bảo vệ trước các mối nguy cơ từ mã độc, như việc mã độc muốn xóa chương trình diệt virus ra khỏi máy tính. Việc bảo vệ được thực hiện trên file của trương trình trên ổ đĩa, trên RAM và trong Registry. - Ngăn chặn tất cả quá trình điều khiển chương trình diệt virus qua máy tính điều khiển từ xa. - Thiết lập Password để bảo vệ chương trình khi muốn truy cập hay thực hiện các tác vụ cụ thể. - Tính năng Phát hiện và ngăn chặn các thiết bị USB mô phỏng giả mạo thiết bị bàn phím (BadUSB Attack Prevention)	
		Chức năng Report: - Hỗ trợ report các thông tin ngay tại máy trạm: Virus quét được; vị trí file nhiễm virus; vị trí file backup; file được backup; trạng thái Start-stop của service theo từng ngày. - Hỗ trợ thống kê, báo cáo tình hình virus trên toàn mạng. - Hỗ trợ thống kê, báo cáo theo lịch	

Hạng mục số	Tên hàng hóa/dịch vụ liên quan	Thông số kỹ thuật và các tiêu chuẩn	Yêu cầu khác
		- Hỗ trợ báo cáo, thống kê tình hình cài đặt, trạng thái update virus trên toàn mạng - Hỗ trợ xuất báo cáo qua nhiều dạng khác nhau PDF, XLS,… + các báo cáo phải được phân loại theo mức độ quan trọng. + các thông báo hệ thống được thực hiện dưới dạng Pop-up trên thanh Taskbar. + Hiển thị nhiều thông tin trên Dashboard. + Các cảnh báo có thể thực hiện qua: Email	
		Quản lý tập trung: - Phần mềm quản trị tập trung hỗ trợ cài đặt trên các hệ điều hành: Server 2008 SP1, Server 2012, Server 2016, Server 2019, Server 2022, Server 2025 - Phần mềm quản trị tập trung cho phép triển khai phân cấp theo cơ chế Master/ Slave để phù hợp với các tổ chức lớn. - Giao diện phần mềm quản trị có thể cài đặt trên Window, Linux. Hỗ trợ giao diện theo chuẩn MMC của Microsoft và giao diện Web. - Giám sát việc sử dụng dịch vụ đám mây (Cloud Discovery only). - Hỗ trợ gỡ bỏ các phần mềm từ xa trên các máy Client. - Quản lý phần cứng dựa trên các thông tin trên Registry. - Có tính năng quản lý moblie android, IOS - Cho phép phản ứng tự động khi phát hiện virus vượt quá giới hạn - Giải pháp chỉ cần một Agent chạy duy nhất quản lý cho các module của chương trình.	

Hạng mục số	Tên hàng hóa/dịch vụ liên quan	Thông số kỹ thuật và các tiêu chuẩn	Yêu cầu khác
		- Giải pháp phải có khả năng tập trung quản lý, triển khai, báo cáo. - Khả năng phân chia nhóm quản lý và thiết lập các chính sách quản lý khác nhau. - Giải pháp có khả năng cho phép người quản trị kiểm soát ngăn ngừa việc sử dụng License phần mềm Antivirus một cách trái phép. - Khả năng thiết lập cấu hình Anti-virus, Firewall tới từng máy trạm từ xa và không cho phép người sử dụng bình thường thay đổi các thiết lập này. - Hỗ trợ báo cáo, thống kê tình hình cài đặt, trạng thái update virus trên toàn hệ thống. - Chức năng quản lý, áp dụng chính sách không phụ thuộc vào Active Directory. - Cho phép người dùng có thể điều khiển được phần mềm diệt virus khi ra khỏi mạng.	
		Khả năng cung cấp tính năng phân tích điều tra nguồn gốc tấn công: - Cung cấp khả năng hiển thị rõ ràng hơn về các đối tượng độc hại bằng "thẻ sự cố", mô tả chi tiết quá trình lây nhiễm, với đường lây lan của đối tượng, liệt kê các dữ liệu được thu thập trong thẻ sự cố như: registry, file drop, network - Xem toàn bộ phạm vi của bất kỳ mối đe dọa nào. Hiểu nguyên nhân gốc rễ của mối đe dọa và cách nó thực sự xảy ra. Tìm ra đợt tấn công bắt đầu từ đâu? khi nào? mối đe dọa này có còn đang ẩn nấp ở đâu? để loại bỏ các gốc rễ của cuộc tấn công đó	
2	Cập nhật license phần mềm	- Cập nhật license trên các máy chủ, máy trạm tại Trụ sở Bộ, Số 8 Tôn Thất Thuyết, Cầu Giấy Hà Nội.	

Hạng mục số	Tên hàng hóa/dịch vụ liên quan	Thông số kỹ thuật và các tiêu chuẩn	Yêu cầu khác
		- Cài đặt, cấu hình máy chủ quản lý tập trung, thiết lập chính sách, tác vụ quản lý các endpoint.	

Phần 2: Mua 01 năm bản quyền cập nhật phần mềm Mail-SeCure cho hệ thống thư điện tử công vụ

Hạng mục số	Tên hàng hóa/dịch vụ liên quan	Thông số kỹ thuật và các tiêu chuẩn	Yêu cầu khác
1	Mua 01 năm bản quyền cập nhật phần mềm Mail-SeCure cho hệ thống thư điện tử công vụ	- Cập nhật các bản vá/sửa lỗi (Bug fixes, Feature upgrades, Major releases...) - Nâng cấp phiên bản mới cho hệ điều hành và phần mềm (Version Upgrade) - Cập nhật các hình thức chống tấn công vào email gateway mới. - Hỗ trợ kỹ thuật từ hãng.	
2	Hỗ trợ kỹ thuật	- Kiểm tra tình trạng hoạt động của phần mềm. - Kiểm tra, rà soát nhật ký hệ thống. - Nâng cấp phần mềm, hotfix cho phần mềm. - Cập nhật tính năng bảo mật (Signature, Patten). - Sao lưu cấu hình, chính sách hiện tại của phần mềm.	
3	Xử lý sự cố	- Thời gian sẵn sàng: 24h x 7 ngày /tuần. - Thời gian phản hồi: 1 giờ - Thời gian đáp ứng: 4 giờ - Chịu trách nhiệm khôi phục hệ thống bị hỏng do lỗi phần cứng, phần mềm trong thời gian ngắn nhất.	

Mục 2. Bản vẽ

Không có bản vẽ.

Mục 3. Kiểm tra và thử nghiệm

Các kiểm tra và thử nghiệm cần tiến hành gồm có: Kiểm tra chạy thử khi cập nhật License phần mềm.