Phụ lục

YÊU CẦU KỸ THUẬT

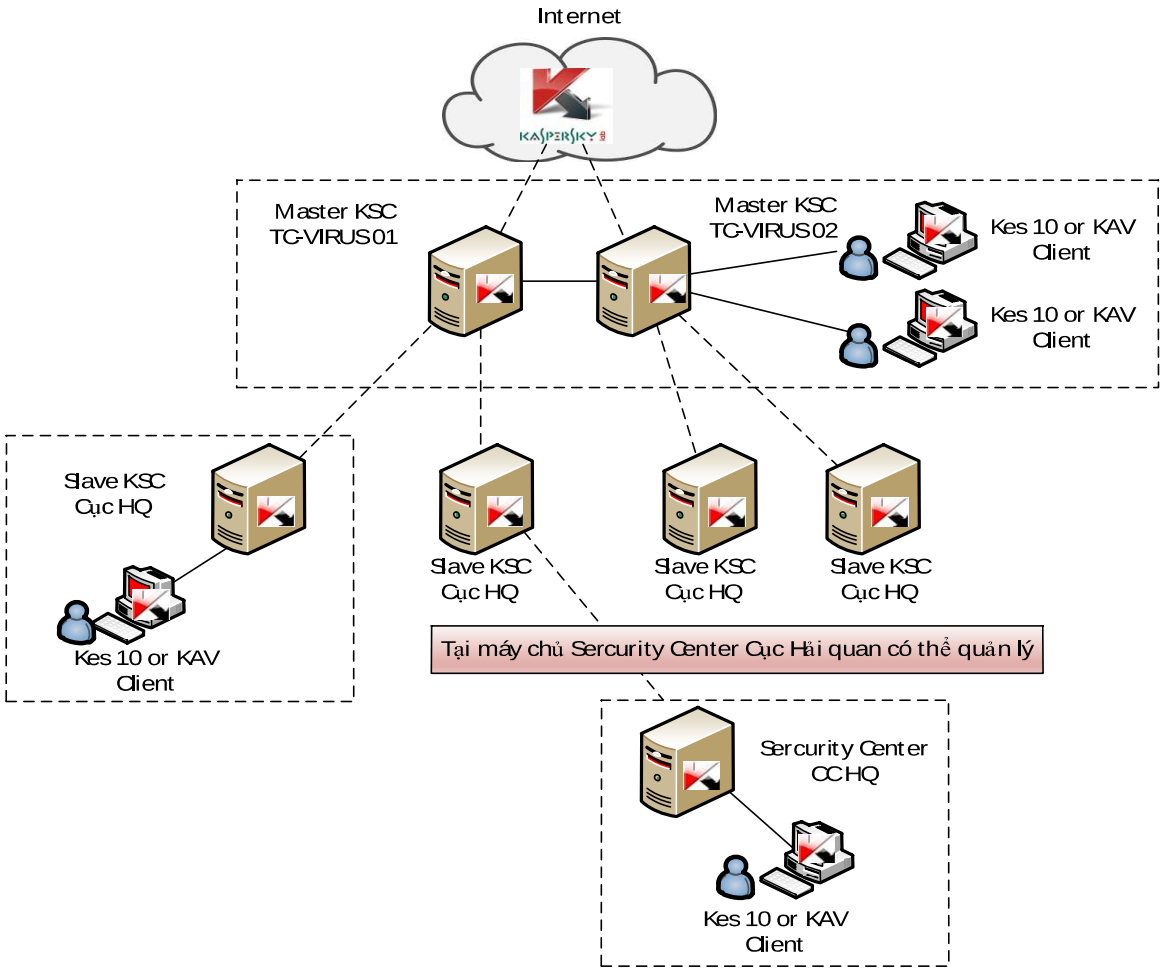
(Kèm theo Công văn số 98 /CNTT-TH ngày 09 / 4 /2025 của Ban Công nghệ thông tin và Thống kê hải quan)

1. Hiện trạng bộ phần mềm Antivirus Kaspersky đang được sử dụng:

Hiện nay, hầu hết các máy trạm, máy chủ đang hoạt động trên mạng trong toàn ngành Hải quan được trang bị tập trung phần mềm diệt virus của hãng Kaspersky (trừ các máy sử dụng Hệ điều hành Unix). Mô hình triển khai phần mềm AntiVirus Kaspersky ngành Hải quan là mô hình quản trị tập trung với máy chủ Master tại Cục Hải quan và phân cấp quản lý với các máy chủ Slave tại các Cục/Chi cục Hải quan; quản lý License tập trung tại máy chủ Master cấp Cục. Thông qua hệ thống quản trị tập trung, cán bộ quản trị có thể thực hiện:

- Cài đặt tự động phần mềm AntiVirus cho người dùng cuối;
- Thiết lập các chính sách về bảo vệ, chính sách về cập nhật, nâng cấp;
- Cấp phát và quản lý License tự động;
- Tự động sinh ra các báo cáo về tình hình hoạt động.

Mô hình triển khai hệ thống Kaspersky của Cục Hải quan thực hiện theo mô hình phân cấp Master - Slave. Hai máy chủ Master Kaspersky Security Center (KSC hay có thể gọi là máy chủ Admin Kit) đặt tại Cục có khả năng quản lý một hoặc nhiều máy chủ KSC và Clients tại các đơn vị Hải quan địa phương. Mô hình hệ thống:



Giải thích các thành phần thuộc mô hình

■ Internet:

• Môi trường kết nối để KSC Master có thể kết nối tới máy chủ Kaspersky Lab phục vụ việc cập nhật.

■ KSC Master:

• Kết nối tới máy chủ Kaspersky Lab để tải về cập nhật cơ sở dữ liệu virus và các phiên bản mới của KES, KSC. Phiên bản được KSC tại Cục và cục đang chạy là KSC 11.x.x

• Quản trị các máy chủ KSC Slave.

■ KSC Slave:

• Kết nối tới máy chủ Kaspersky Master để tải về cập nhật cơ sở dữ liệu virus và các phiên bản mới của KES, KSC.

• Cập nhật cơ sở dữ liệu virus và quản trị các máy trạm.

■ Client:

• Các máy trạm được cài đặt Kaspersky Endpoint Security 11.x.x (KES 11)

Hai máy chủ KSC ở chế độ Master quản lý trực tiếp các máy chủ KSC tại

các Cục. KSC tại Cục kết nối và chịu sự quản lý từ KSC Master tại Cục Hải quan. Các Chi cục có triển khai KSC và Update Agent trung tâm miền thông qua KSC tại Cục.

Các máy trạm được quản lý theo kiến trúc của hệ thống AD, phân cấp theo các OU/Cục - Chi cục.

Kaspersky tại cấp:	**Số lượng**	**Chức năng**	**Phiên bản**
KSC Master	2	- Quản lý các máy chủ KSC slave. - Quản lý các máy chủ/ máy trạm tại Cục	Kaspersky Security Center 11.x.x
KSC slave tại Cục	35	Quản lý máy chủ/ máy trạm tại cấp Cục/ Chi cục Hải quan	Kaspersky Security Center 11.x.x
Client	~1.000 Server và 9.441 PC (trên phần mềm QLTS)	Update từ KSC	Kaspersky Endpoint Security 11.x.x

2. Yêu cầu về cấu hinh kỹ thuật và triển khai:

2.1. Yêu cầu về kỹ thuật nội dung mua sắm

- Mua gia hạn bản quyền phần mềm (license) Antivirus Kaspersky sử dụng cho hệ điều hành Windows, Linux để thực hiện triển khai cho các đơn vị trong toàn ngành

License Antivirus Kaspersky
- Hỗ trợ hệ điều hành: Windows, Linux - Tính năng Anti-Malware: cho File, Email, Web; - Các tính năng Endpoint: + Tường lửa cá nhân: Firewall; + Phòng chống tấn công: IPS hoặc Network Attack Blocker; HIPS hoặc Host Intrustion Prevention; + Kiểm soát thiết bị: Device Control; + Kiểm soát truy nhập Web:Web Control;

+ Kiểm soát ứng dụng: Application Control; - Tính năng quản trị tập trung: quản trị chính sách - Policy, quản trị lập lịch – Task, quản trị thiết bị - Device; - Tính năng lập báo cáo, thống kê tình hình mã độc. - Số lượng License: 9.000, quản trị tập trung tại Cục Hải quan; - Bảo hành (hỗ trợ kỹ thuật) trong thời gian sử dụng (02 năm) theo tiêu chuẩn của nhà sản xuất.

- Dịch vụ triển khai.

2.2. Các nội dung triển khai

2.2.1. Yêu cầu chung về triển khai

- Triển khai không được ảnh hưởng hoặc gián đoạn đến vận hành của các hệ thống công nghệ thông tin (máy chủ, máy trạm, chương trình ứng dụng).

- Đội ngũ cán bộ triển khai của nhà thầu phải có chứng chỉ theo yêu cầu của HSMT. Trong quá trình nhà thầu triển khai phải có sự tham gia và hỗ trợ kỹ thuật của cán bộ kỹ thuật của hãng sản xuất sản phẩm chào thầu. Trước thời điểm xây dựng quy trình chi tiết, nhà thầu phải cung cấp thư hoặc tài liệu của đại diện nhà sản xuất (theo định nghĩa về đại diện nhà sản xuất tại HSMT) có nội dung xác nhận về việc cử cán bộ kỹ thuật của hãng sản xuất tham gia hỗ trợ kỹ thuật trong quá trình triển khai.

2.2.2. Yêu cầu về khảo sát:

- Khảo sát hiện trạng của hệ thống diệt Virus hiện tại của Cục Hải quan.

- Xây dựng báo cáo khảo sát chi tiết.

2.2.3. Yêu cầu về triển khai:

- Căn cứ hàng hóa chào thầu và giải pháp đề xuất tại HSDT, nhà thầu thực hiện xây dựng tài liệu triển khai chi tiết gồm:

- Xây dựng quy trình nâng cấp, cập nhật hệ thống diệt Virus hiện tại lên phiên bản mới nhất (nếu có hoặc nếu tương thích) đối với máy chủ quản trị và máy đầu cuối;

- Xây dựng quy trình cập nhật, kiểm tra License vào hệ thống;

- Thực hiện triển khai hệ thống theo tài liệu quy trình đã được phê duyệt;

-Thực hiện kiểm tra hệ thống sau triển khai, đảm bảo hoạt động đúng theo tài liệu đã được Chủ đầu tư phê duyệt;

- Lập tài liệu hoàn công hệ thống; tài liệu hướng dẫn quản trị, vận hành hệ thống.

- Xây dựng quy trình và hỗ trợ bên mua thực hiện chuyển đổi 35 KSC Slave theo mô hình tổ chức cũ về 20 KSC Slave tại 20 Chi cục Hải quan khu vực theo mô hình tổ chức mới; quy trình chuyển đổi kết nối máy trạm/máy chủ theo mô hình 35 KSC Slave cũ về 20 KSC Slave mới tương ứng khi Cục Hải quan thực hiện tổ chức lại mô hình công nghệ thông tin

2.2.4. Yêu cầu hỗ trợ kỹ thuật trong thời gian hiệu lực License:

- Cung cấp đầu mối, nhân sự hỗ trợ kỹ thuật trực tiếp tại Cục Hải quan khi có sự cố hoặc nguy cơ bùng phát Virus trong suốt thời gian License có hiệu lực.