YÊU CẦU VỀ KỸ THUẬT (Chương V, E-HSMT)

1. Giới thiệu chung về dự án, gói thầu:

- Chủ đầu tư: Đài Phát thanh và Truyền hình Thành Phố Hồ chí Minh

- Địa chỉ: số 9 Nguyễn Thị Minh Khai, phường Sài Gòn, TP. Hồ Chí Minh.

- Điện thoại: (028) 38.297714 Fax: (028) 39.103082

- Tên gói thầu: K02-25: Mua license, phần mềm hỗ trợ kỹ thuật các hệ thống công nghệ thông tin

- Quy mô đầu tư: cung cấp license, phần mềm hỗ trợ kỹ thuật các hệ thống công nghệ thông tin

- Vị trí lắp đặt : tại Đài Phát thanh và truyền hình Thành Phố Hồ chí Minh

- Thời gian thực hiện gói thầu: năm 2025-2026

2. Mục tiêu công việc:

Nhằm đảm bảo an toàn, an ninh thông tin cho các hệ thống công nghệ thông tin của Đài.

3. Yêu cầu kỹ thuật của gói thầu:

a. Yêu cầu về kỹ thuật chung :

- Hàng hóa phải hợp lệ theo yêu cầu tại E-CDNT 10.8 Bảng dữ liệu đấu thầu.

- Hàng hóa được đóng gói theo đúng tiêu chuẩn của nhà sản xuất, phù hợp với điều kiện vận chuyển để đảm bảo không bị hư hỏng trong quá trình vận chuyển.

- Hàng hóa khi cung cấp cho Chủ đầu tư phải có đầy đủ catalog, tài liệu kỹ thuật chi tiết, hướng dẫn sử dụng ... theo tiêu chuẩn của nhà sản xuất, đảm bảo việc kiểm tra, thử nghiệm.

- Mọi thiết bị không đạt tiêu chuẩn đưa vào trong hồ sơ dự thầu có thể dẫn đến loại bỏ hồ sơ dự thầu và nhà thầu phải chịu hoàn toàn trách nhiệm về việc làm của mình.

b. Yêu cầu kỹ thuật cụ thể

Yêu cầu về kỹ thuật cụ thể như tính năng, thông số kỹ thuật, các bản vẽ, catalô, các thông số bảo hành… được nêu cho từng loại hàng hóa **được mô tả theo bảng dưới đây. Trong E-HSDT, Nhà thầu phải nộp một Bảng đề xuất kỹ thuật thể hiện chi tiết thông số, tính năng kỹ thuật để cam kết, chứng minh hàng hóa do nhà thầu chào tuân thủ, đáp ứng tất cả các yêu cầu kỹ thuật này:**

Hạng mục số	Tên dịch vụ liên quan	Thông số kỹ thuật và các tiêu chuẩn
	Đặc tính, thông số kỹ thuật, tiêu chuẩn kỹ thuật của hàng hóa	
A	**Hàng hóa**	
1	Chứng thư số (SSL) cho hệ thống web, mail (thời hạn 2 năm)	Chứng thư số xác thực tổ chức và bảo mật cho hệ thống của doanh nghiệp Tên miền sử dụng: *.htv.com.vn Tiêu chuẩn kỹ thuật Chứng thư số: - Wildcard SSL (2 năm) - Mã hóa đến 256 bits-Phương thức chứng thực: Chứng thực doanh nghiệp (OV) - Mã hóa công khai ECC - Quản lý chứng thư số trực tiếp thông qua hệ thống control panel - Không giới hạn thay đổi tên miền sử dụng - Đồng bộ thời hạn hết hạn của chứng thư số tại 1 thời điểm - Hỗ trợ tùy chọn mở rộng SANs - Không giới hạn cặp khóa (Keypair) cho server sử dụng - Hỗ trợ tất cả subdomain level 1 của *.htv.com.vn - Hỗ trợ cấp phát lại, cấp mới trong vòng 5 – 10 phút sau khi xác thực và kiểm duyệt thông tin tổ chức - Hỗ trợ và khắc phục sự cố trong vòng 24h - Miễn phí cấp phát lại chứng chỉ trong suốt thời gian hiệu lực - Tương thích với mọi trình duyệt phổ biến - Không giới hạn số lượng máy chủ cài đặt
2	Bản quyền (license) phần mềm diệt virus cho máy trạm (thời hạn 2 năm)	Hỗ trợ các tính năng sau: - Bảo mật cho Web (Web Security) - Đánh giá mức độ uy tín của việc download từ các trang web (Download Reputation) - Khả năng lọc địa chỉ web theo phân mục định nghĩa sẵn (Web Control / Category-based URL Blocking)

		- Quản lý thiết bị cắm vào máy trạm (Peripheral Control) - Khả năng ngăn chặn thất thoát dữ liệu (Data Loss Prevention) - Sử dụng công nghệ máy học – Deep learning, để phân tích và phát hiện mã độc - Khả năng ngăn chặn phần mềm độc hại (Anti-Malware File Scanning) - Bảo vệ theo thời gian thực (Live Protection) - Khả năng phân tích hành vi trước khi thực thi của mã độc (Pre-execution Behavior Analysis) - Chống xâm nhập - HIPS (Host Intrusion Prevention System) - Khả năng phát hiện và ngăn chặn các phần mềm không mong muốn Potentially Unwanted Application (PUA) Blocking - Ngăn chặn các hình thức tấn công khai thác, xâm nhập (Exploit Prevention) - Có khả năng phân tích hành vi của ứng dụng đang hoạt động để phát hiện mã độc (Runtime Behavior Analysis) - Sử dụng công nghệ Anti-Malware Scan Interface (AMSI) để phát hiện mã độc - Khả năng phát hiện các luồng dữ liệu độc hại (Malicious Traffic Detection (MTD)) - Ngăn chặn virus mã hóa dữ liệu anti-ransomeware (CryptoGuard Ransomware Protection) - Ngăn chặn mã độc xâm nhập Ổ cứng và phần vùng hệ điều hành (Wipeguard) - Khả năng tự động loại bỏ các malware (Automated Malware Removal) - Khả đồng bộ tín hiệu an ninh thông tin giữa máy trạm và thiết bị firewall gateway (Synchronized Security Heartbeat) - Khả năng phân tích nguồn gốc của vấn đề an ninh thông tin (Root Cause Analysis) - Giao diện quản lý điện toán đám mây thông qua nền tảng web-base

		- Quản trị tập trung hệ thống bảo mật cho máy trạm, máy chủ, và thiết bị di động qua hệ thống đám mây (cloud central managed) - Khả năng mở rộng quản lý chung các hệ thống bảo mật trên một giao diện Web, gồm: Email Gateway, Wireless, Firewall, Device Encryption - Hỗ trợ đặt mật khẩu chống gỡ cài đặt (Tamper Protection) - Khả năng tự động đồng bộ với Microsoft Active Directory (Automatic Active Directory synchronization) - Khả năng tự động ưu tiên các báo động của hệ thống (Automatically prioritized alerts) - Phân quyền quản lý theo vai trò, cấp bậc (Administration Roles): Super Admin, Admin, help Desk, Read Only - Hỗ trợ API - Có thể tạo chính sách quản lý riêng biệt cho từng user (Granular, per-user policy management) - Cùng hãng sản xuất hoặc tương thích với phần mềm Sophos đang sử dụng hiện tại. - Thời hạn sử dụng: 2 năm
3	Bản quyền (license) phần mềm diệt virus cho máy chủ (thời hạn 2 năm)	- Hỗ trợ hệ điều hành: o Windows Server 2016, 2019, 2022 o Linux: Amazon Linux, Amazon Linux 2, CentOS 7/8, Debian 9, 10, Oracle Linux 7/8, Red Hat Enterprise Linux 7/8/9, SUSE 12/15, Ubuntu 18/20.04/22.04 LTS o Cloud Workload Flatform: AWS, MS Azure, Google Cloud - Bảo mật cho Web (Web Security) - Đánh giá mức độ uy tín của việc download từ các trang web (Download Reputation) - Khả năng lọc địa chỉ web theo phân mục định nghĩa sẵn (Web Control / Category-based URL Blocking) - Quản lý thiết bị cắm vào máy trạm (Peripheral/Device Control)

		- Khả năng quản lý các ứng dụng cài đặt tại máy trạm (Application Control) - Cho phép thiết lập danh sách ứng dụng tin tưởng trên máy chủ (Server Lockdown) - Khả năng ngăn chặn thất thoát dữ liệu (Data Loss Prevention) - Sử dụng công nghệ máy học – Deep learning, để phân tích và phát hiện mã độc - Khả năng ngăn chặn phần mềm độc hại (Anti-Malware File Scanning) - Bảo vệ theo thời gian thực (Live Protection) - Khả năng phân tích hành vi trước khi thực thi của mã độc (Pre-execution Behavior Analysis) - Chống xâm nhập - HIPS (Host Intrusion Prevention System) - Khả năng phát hiện và ngăn chặn các phần mềm không mong muốn (Potentially Unwanted Application (PUA) Blocking) - Ngăn chặn các hình thức tấn công khai thác, xâm nhập (Exploit Prevention) - Có khả năng phân tích hành vi của ứng dụng đang hoạt động để phát hiện mã độc (Runtime Behavior Analysis) - Sử dụng công nghệ Anti-Malware Scan Interface (AMSI) để phát hiện mã độc - Khả năng phát hiện các luồng dữ liệu độc hại (Malicious Traffic Detection (MTD)) - Ngăn chặn virus mã hóa dữ liệu anti-ransomeware (CryptoGuard -Ransomware File Protection) - Ngăn chặn mã độc xâm nhập Ổ cứng và phân vùng hệ điều hành (Wipeguard) - Khả năng tự động loại bỏ các malware (Automated Malware Removal) - Khả đồng bộ tín hiệu an ninh thông tin giữa máy trạm và thiết bị firewall gateway (Synchronized Security Heartbeat) - Giám sát tính toàn vẹn của tập tin trong hệ thống (File Integrity monitoring) - Khả năng phân tích nguồn gốc của vấn đề an ninh thông tin (Root Cause Analysis)

		- Hệ thống quản lý nền tảng đám mây - Giao diện quản lý điện toán đám mây thông qua nền tảng web-base - Quản trị tập trung hệ thống bảo mật cho máy trạm, máy chủ, và thiết bị di động qua hệ thống đám mây (cloud central managed) - Khả năng mở rộng quản lý chung các hệ thống bảo mật trên một giao diện Web, gồm: Email Gateway, Wireless, Firewall, Device Encryption - Hỗ trợ đặt mật khẩu chống gỡ cài đặt (Tamper Protection) - Khả năng tự động đồng bộ với Microsoft Active Directory (Automatic Active Directory synchronization) - Khả năng tự động ưu tiên các báo động của hệ thống (Automatically prioritized alerts) - Phân quyền quản lý theo vai trò, cấp bậc (Administration Roles): Super Admin, Admin, help Desk, Read Only - Hỗ trợ API - Có thể tạo chính sách quản lý riêng biệt cho từng Server - Cùng hãng sản xuất hoặc tương thích với phần mềm Sophos đang sử dụng hiện tại. - Thời hạn sử dụng: 2 năm
4	Bản quyền phần mềm và hỗ trợ hệ thống tường lửa Fortigate FG 800D hiện hữu (thời hạn 2 năm)	Bản quyền các dịch vụ bao gồm: - Dịch vụ cập nhật cơ sở dữ liệu chống Virus, - chống tấn công xâm nhập, - Dịch vụ chống tấn công phần mềm độc hại nâng cao, phân tích mã độc trên điện toán đám mây - Dịch vụ nhận diện ứng dụng truy cập, - Dịch vụ lọc dữ liệu truy cập web, - Dịch vụ hỗ trợ kỹ thuật đáp ứng SLA 24x7 của hãng : hỗ trợ thông qua web chat, qua điện thoại, hoặc tạo ticket - Dịch vụ cập nhật, nâng cấp firmware, bảo hành và thay thế phần cứng - Cùng hãng sản xuất hoặc tương thích với hệ thống tường lửa Fortigate FG800D đang sử dụng hiện tại. - Thời hạn sử dụng: 2 năm

5	Bản quyền (license) phần mềm Microsoft 365 bản Basic (Microsoft 365 Business Basic) (thời hạn 2 năm)	- Phiên bản web và di động của Word, Excel, PowerPoint, và Outlook - Chat, gọi, họp trực tuyến lên đến 300 người tham gia - Dung lượng lưu trữ đám mây 1 TB cho mỗi người dùng - Email doanh nghiệp 50GB - Quản lý lịch hẹn khách hàng - Bảo mật tiêu chuẩn - Hỗ trợ điện thoại và web bất kỳ lúc nào - Dịch vụ đám mây bảo mật: Microsoft Teams, OneDrive, SharePoint, Exchange - Thời hạn sử dụng: 2 năm
6	Gia hạn license cho hệ thống lưu trữ hiện hữu Nutanix NX-1175S-G7: Gia hạn bản quyền phần mềm (NCI Starter), theo số lượng core (thời hạn 2 năm)	Hỗ trợ các tính năng: - Hệ điều hành Acropolis (AOS) - Hypervisor AHV (Acropolis Hypervisor) - Prism Element - Prism Central - Dịch vụ lưu trữ phân tán - Nén dữ liệu cơ bản (Basic Compression - LZ4) - Chống trùng lặp dữ liệu (Data Deduplication - Inline) - Snapshots và Clones - Volume Groups for in-cluster VMs - Dự phòng đường dẫn dữ liệu (Data Path Redundancy) - Hệ số dự phòng (Redundancy Factor - RF2) - Khả năng phục hồi cấp node (Node-level Availability Domains) - Phục hồi thảm họa cơ bản (Basic Disaster Recovery) - Thời hạn sử dụng: 2 năm
7	Bản quyền (license) Symantec cho hệ thống làm tin iNews hiện hữu (thời hạn 2 năm)	Hỗ trợ các tính năng sau: Antivirus | Diệt virus - Diệt virus và mã độc trên các máy trạm và máy chủ được cài đặt SEP. - Phát hiện và diệt các phần mềm gián điệp trên máy tính. - Đặt lịch quét tự động một phần hoặc toàn bộ trên các máy trạm.

		Firewall | Tường lửa bảo mật - Triển khai các rule, thông báo tương ứng với các hành động trên máy trạm. - Phân tích và lọc các traffic độc hại. - Ngăn chặn hoặc cho phép các kết nối qua các port, các giao thức mạng. Application and Device Controll | Kiểm soát thiết bị và ứng dụng - Chặn hoặc cho phép các ứng dụng có trên máy trạm theo đường dẫn hoặc file chạy của ứng dụng. - Chặn hoặc cho phép kết nối các thiết bị ngoại vi như USB, máy in, chuột, bàn phím… - Ghi lại log của các lần kết nối và lưu trữ log tại máy chủ SEPM. Host Intrusion Prevention | Chống tấn công chủ động - Sử dụng nguồn là các dữ liệu bảo mật mà người dùng trên toàn cầu chia sẻ để đưa ra các đánh giá phân tích về đối tượng nghi vấn. Từ đó đưa ra hành động trước khi đối tượng có thể gây hại cho máy tính của bạn. - Ngăn chặn malware, mã độc trước khi chúng tấn công máy tính của bạn. Live Update | Cập nhật tập trung - Các bản cập nhật dữ liệu về các mẫu virus mới có thể tùy chỉnh chế độ cập nhật. - Các máy trạm có thể cập nhật trực tiếp từ internet là máy chủ của Symantec. - Hoặc có thể được cập nhật về duy nhất máy chủ quản trị tập trung SEPM. Các máy trạm sẽ cập nhật dữ liệu từ máy chủ SEPM mà không cần truy cập ra internet. Giúp tiết kiệm và giảm băng thông internet của toàn hệ thống. - Đặt lịch cập nhật tự động trên các máy trạm. Report | Báo cáo

		- Báo cáo đầy đủ và chi tiết về tình trạng của hệ thống, vấn đề bảo mật tại các máy trạm. - Cơ chế tìm kiếm báo cáo cho một vài máy trạm chỉ định. - Có thể đặt lịch để xuất các báo cáo tự động và gửi email cho quản trị viên. - Cùng hãng sản xuất hoặc tương thích với phần mềm Symantec đang sử dụng hiện tại. Thời hạn sử dụng: 2 năm
8	Bản quyền (license) phần mềm diệt virus cho máy tính Trung tâm dịch vụ (thời hạn 2 năm)	Hỗ trợ nhiều công nghệ bảo vệ chống mã độc, mối đe dọa như: - Máy học độ tin cậy cao (high-fidelity machine learning) - Phân tích hành vi - Ngăn ngừa các biến thể mã độc (variant protection), - Kiểm tra độ tin cậy của mẫu (census check), - Kiểm soát ứng dụng, - Ngăn chặn khai thác trong tài liệu (exploit prevention), - Ransomware rollback - Độ nổi tiếng của các web (web reputation), - Kiểm soát kết nối tới C&C - Chặn thất thoát dữ liệu - Khả năng ngăn chặn các ransomware tinh vi mã hóa file trên các thiết bị đầu cuối, có thể chặn các hành vi mã hóa nguy hiểm, và phục hồi các file đã bị mã hóa nếu cần thiết - Cho phép nhận thông tin chia sẻ về hiểm họa (threat intelligence) từ nguồn khác thông qua: TAXII và MISP - Cho phép tùy biến dashboard phù hợp dựa trên vai trò quản trị khác nhau. - Hỗ trợ bảo vệ đa nền tảng như: Windows, Linux, MAC OS. Yêu cầu về tính năng bảo mật – phát hiện mối đe dọa - Tính năng phát hiện mã độc sử dụng công nghệ máy học với độ tin cậy cao ở cả hai

		mức độ trước thực thi (pre-execution) và thực thi (runtime): - Pre-Execution Machine Learning (công nghệ học máy ở giai đoạn tiền thực thi) - Runtime Machine Learning (công nghệ học máy ở giai đoạn thực thi) Tính năng phân tích hành vi, dùng để ngăn chặn dạng tấn công sau: - Sử dụng script khai thác - Injection - Ransomware - Memory attacks - Browser attacks - Hỗ trợ bảo vệ ứng dụng AI. Giải pháp có thể nhận dạng được các ứng dụng nghi ngờ hoặc không tin cậy cố gắng thay đổi các file của ứng dụng AI trên máy tính - Tính năng kiểm tra độ nổi tiếng của file (File Reputation), độ nổi tiếng của web (Web Reputation), bảo vệ phát hiện các biến thể mã độc mới… Tính năng ngăn chặn tấn công khai thác (host firewall, exploit protection): - Host firewall - Exploit protection Kiểm soát thiết bị ngoại vi – device control dựa trên nhiều tiêu chí: - Location awareness: theo vị trí của máy trạm - Áp dụng tới từng người dùng, nhóm người dùng, có thể kết nối với Active Directory - Block autorun - Hỗ trợ cả mobile device, CD/DVD, Floppy disk, network drives, USB storage devices, thiết bị giao tiếp hồng ngoại, bluetooth Chính sách cho device control hỗ trợ nhiều action như: - Full access - Modify - Read and execute

		- Read - List device content only - Block - Tính năng Update Agent: cho phép lựa chọn một số agent làm thành phần cache các thông tin cập nhật như pattern, engine. Các agent chỉ cần cập nhật từ thành phần update agent này giúp giảm lưu lượng cập nhật trực tiếp từ server - Tính năng kiểm soát các dữ liệu - Cung cấp chính sách kiểm soát, ngăn chặn thất thoát dữ liệu quan trọng trực tiếp trên các nhóm máy tính xách tay hoặc từng máy tính xách tay cụ thể - Cung cấp khả năng kiểm soát, ngăn ngừa nguy cơ thất thoát dữ liệu quan trọng từ các máy tính xách tay thông qua các kênh truyền: email client, web mail, SMB, HTTP/HTTPs, ứng dụng IM, ứng dụng Peer-to-Peer, cloud storage… - Cho phép cấu hình kiểm soát nguy cơ thất thoát dữ liệu quan trọng qua các thiết bị ngoại vi: CD/DVD, máy in, USB… Cho phép định nghĩa những dữ liệu quan trọng dựa trên kết hợp nhiều thông số: - Biểu thức, cấu trúc dữ liệu. Ví dụ: Số thẻ tín dụng… - Thuộc tính của file: loại file và kích thước file - Từ khóa (keyword) - Cho phép định nghĩa, áp dụng chính sách riêng biệt cho thiết bị máy tính xách tay ở Internal (tại văn phòng Tổ chức) và External (tại nhà, khu vực khác) - Cung cấp sẵn các template sẵn có giúp Tổ chức có thể nhanh chóng đáp ứng tuân thủ với các bộ nguyên tắc như: PCI/DSS, HIPAA, GLBA … - Yêu cầu về tính năng vá ảo bảo vệ trước các hành vi khai thác, tấn công - Hỗ trợ nhanh chóng các bản vá ảo lỗ hổng bảo mật cho máy trạm.

		- Ngăn chặn các khai thác lỗ hổng zero-day cho máy trạm trong mạng hoặc ngoài mạng của tổ chức - Cung cấp các bản vá ảo nghiêm trọng cho các hệ điều hành không còn được hỗ trợ bởi chính hãng thông qua các rule bảo vệ bởi module host based IPS - Yêu cầu về tính năng giám sát ứng dụng - Cho phép tổ chức nâng cao khả năng phòng thủ chống lại mã độc và các cuộc tấn công có chủ đích (Advanced persistent threat-APT) bằng cách ngăn chặn các ứng dụng không biết/không mong muốn thực thi trên máy trạm bằng sử dụng chính sách động kết hợp whitelist và blacklist - Ngăn chặn các tác động nguy hiểm từ các ứng dụng không mong muốn/không biết thông qua kiểm soát các file thực thi (đường dẫn file, mã hash…), danh mục các ứng dụng trên endpoint, certificate cho cả whitelist/allow list và blacklist/block list - Cho phép lockdown hệ thống để khóa người dùng không cho phép thực thi các ứng dụng mới. - Yêu cầu về tính năng điều tra và phản hồi (XDR) - Nền tảng XDR cùng với sensor chuyên dụng (native sensor). Ngoài endpoint, giải pháp còn hỗ trợ thu thập và tương quan dữ liệu từ nhiều nguồn khác nhau chẳng hạn như email, server, network… - Áp dụng AI và phân tích chuyên sâu để phân tích các dữ liệu từ các cảm biến sensor chuyên dụng (native sensor) để đưa ra các cảnh báo độ tin cậy cao - Hỗ trợ sẵn ASRM và Zero Trust trong cùng một hệ quản trị với XDR - XDR agent có khả năng kiểm tra các build/version của Windows tối thiểu mỗi 10 phút, hoặc ngay khi máy trạm Windows thực hiện cập nhật - Có khả năng phát hiện các mối đe dọa bảo mật tồn tại trong hệ thống. Đánh giá dựa

		vào các xu thế mối đe dọa trên phạm vi toàn cầu (chẳng hạn như OpenSSL vulnerability, Samba Linux, Log4Shell Linux/Windows/macOS). Đánh giá rủi ro cloud mailbox, Đánh giá rủi ro máy trạm, máy chủ - Hỗ trợ các phản hồi gồm có: - Thêm/bỏ đối tượng nguy hiểm vào/ra khỏi block list - Thu thập file để điều tra - Isolate endpoint - Chạy custom script (powershell hoặc shell) - Remote shell - Mô hình phát hiện phải kết hợp nhiều quy tắc và bộ lọc bằng cách sử dụng các kỹ thuật như học máy và xếp chồng dữ liệu. Mô hình phát hiện có thể sử dụng một hoặc nhiều bộ lọc để phát hiện các hành vi hoặc sự kiện đáng ngờ và giảm cảnh báo sai (false positive) - Cung cấp danh sách các cảnh báo tương quan chứa tất cả các sự kiện liên quan đến bảo mật được phát hiện trong môi trường của tổ chức. - Danh sách các cảnh báo cho tổ chức có thể điều tra thông qua phân tích nguyên nhân gốc rễ và phân tích chuyên sâu. Hệ quản trị XDR cho phép tổ chức làm giàu thông tin tình báo (custom intelligence) bằng cách nhập thông tin thủ công (import) hoặc tự động từ bên thứ ba. Các loại thông tin được hỗ trợ gồm có - Domain - File (SHA-1, SHA-256, MD5) - File name - IP address - URL - Command line - User account - Định kỳ quét và tìm kiếm các dấu hiệu xâm nhập (Indicator of Compromise) Hỗ trợ quét các dấu hiệu xâm nhập theo mẫu STIX từ bên thứ ba. Hỗ trợ tối thiểu các pattern sau

		- File SHA-1, SHA-256, name-string - Domain name - URL - IP Address (IPv4/Ipv6) - Network traffic - Process (command-line) - User account (account name) - Registry (key, value, type) Hỗ trợ tự động phản hồi cảnh báo với Playbook. Nhà quản trị có thể tự tạo hoặc sử dụng từ mẫu playbook sẵn có của nhà cung cấp Khả năng chia sẻ các đối tượng nghi ngờ cho bên thứ ba tối thiểu gồm có - Palo Alto Panorama - Fortigate NextGen Firewall - CheckPoint Open Platform (OPSEC) Hỗ trợ tích hợp XDR với ứng dụng của bên thứ ba. Tối thiểu gồm có - Microsoft Acitive Directory - Microsoft Entra ID - Q-Radar XDR hoặc Splunk XDR - Elastic - VirusTotal Public API Thời hạn sử dụng: 2 năm
9	Bản quyền (license) phần mềm GoodSync Workstation Runner (thời hạn 2 năm)	Đồng bộ hóa và Sao lưu tệp tin: - Đồng bộ hóa hai chiều (Two-Way Synchronization): GoodSync Workstation Runner có thể đồng bộ hóa các tệp tin và thư mục giữa hai vị trí (ví dụ: giữa máy tính và ổ đĩa ngoài, giữa hai thư mục trên cùng một máy, hoặc giữa máy tính và dịch vụ đám mây). Điều này đảm bảo rằng cả hai vị trí đều có phiên bản tệp tin mới nhất. - Sao lưu một chiều (One-Way Backup): Ngoài đồng bộ hóa, nó cũng hỗ trợ sao lưu một chiều, tức là sao chép tệp tin từ một vị trí nguồn sang một vị trí đích để tạo bản sao dự phòng.

		- Phát hiện và xử lý thay đổi: GoodSync Workstation Runner tự động phát hiện các thay đổi (thêm mới, sửa đổi, xóa) trong các tệp tin và thư mục, sau đó áp dụng những thay đổi đó vào vị trí còn lại để đảm bảo tính nhất quán. Tự động hóa và Lập lịch: - Tự động hóa các tác vụ (Automated Tasks): Cho phép người dùng thiết lập các tác vụ sao lưu và đồng bộ hóa tự động, không cần sự can thiệp thủ công. - Lập lịch (Scheduling): Người dùng có thể lên lịch cho các tác vụ chạy định kỳ (ví dụ: hàng giờ, hàng ngày, hàng tuần) hoặc vào những thời điểm cụ thể. - Đồng bộ hóa theo thời gian thực (Real-Time Synchronization): GoodSync có khả năng đồng bộ hóa ngay lập tức khi phát hiện có sự thay đổi trong tệp tin, đảm bảo dữ liệu luôn được cập nhật. - Chạy nền (Unattended Service/Runner): GoodSync Workstation Runner có thể chạy như một dịch vụ nền, nghĩa là các tác vụ sao lưu và đồng bộ hóa vẫn tiếp tục hoạt động ngay cả khi người dùng không đăng nhập vào hệ thống. Điều này đặc biệt hữu ích cho việc sao lưu máy chủ hoặc các tác vụ quan trọng khác. Hỗ trợ đa dạng các vị trí lưu trữ: - Ổ đĩa cục bộ và mạng nội bộ: Đồng bộ hóa giữa các ổ đĩa cục bộ, ổ đĩa USB, hoặc các thư mục chia sẻ trên mạng nội bộ (LAN). - Dịch vụ đám mây (Cloud Storage): Hỗ trợ tích hợp với nhiều dịch vụ lưu trữ đám mây phổ biến như Google Drive, Dropbox, OneDrive, Amazon S3, Azure Blob Storage, WebDAV, FTP, SFTP, v.v. - NAS (Network Attached Storage): Sao lưu và đồng bộ hóa với các thiết bị NAS. Hiệu suất và Tối ưu hóa:

		- Chuyển đổi dữ liệu cấp khối (Block-Level Data Transfer): GoodSync chỉ truyền tải các khối dữ liệu đã thay đổi thay vì toàn bộ tệp tin, giúp giảm đáng kể thời gian sao lưu, băng thông mạng và yêu cầu lưu trữ. - Chuyển đổi song song (Parallel Threads): Hỗ trợ chạy các tác vụ đồng bộ hóa trong nhiều luồng song song để tăng tốc độ truyền tệp. Kiểm soát và Bảo mật: - Kiểm tra tính toàn vẹn tệp (File Integrity Verification): Có thể so sánh tệp tin bằng mã kiểm tra MD5 hoặc so sánh toàn bộ nội dung tệp để đảm bảo việc sao chép chính xác. - Mã hóa (Encryption): Hỗ trợ mã hóa dữ liệu (ví dụ: AES 256-bit) khi truyền và khi dữ liệu ở trạng thái "at rest" (được lưu trữ). - Xử lý xung đột tự động (Automatic Conflict Resolution): Tự động giải quyết các xung đột khi có sự thay đổi đồng thời trên nhiều vị trí. - Bộ lọc tệp (File Filters): Cho phép người dùng loại trừ hoặc bao gồm các tệp tin và thư mục cụ thể khỏi quá trình đồng bộ hóa dựa trên các tiêu chí như tên, kích thước, hoặc thời gian sửa đổi. - Kiểm soát phiên bản (Versioning): Khả năng giữ lại các phiên bản cũ của tệp tin, cho phép khôi phục lại các phiên bản trước đó nếu cần. Khả năng phục hồi: - Tự động kết nối lại (Automatic Reconnect): Tự động kết nối lại với các thư mục từ xa nếu kết nối bị mất trong quá trình phân tích hoặc đồng bộ hóa. - Ghi nhật ký (Logging): Ghi lại chi tiết các hoạt động, lỗi và thay đổi trong quá trình đồng bộ hóa và sao lưu để người dùng có thể theo dõi và khắc phục sự cố. - Thời hạn sử dụng: 2 năm

10	Bản quyền phần mềm máy chủ FTP (thời hạn 3 năm)	Hỗ trợ các giao thức truyền tệp: - FTP (File Transfer Protocol): Giao thức truyền tệp tin cơ bản và phổ biến nhất. - FTPS (FTP Secure): FTP qua SSL/TLS, cung cấp mã hóa dữ liệu trong quá trình truyền tải để bảo mật thông tin. Đây là tính năng bảo mật cốt lõi của Serv-U FTP Server. - HTTP/HTTPS: Cho phép người dùng truyền tệp thông qua trình duyệt web, thuận tiện cho việc truy cập từ mọi nơi mà không cần cài đặt phần mềm client riêng. Truy cập đa nền tảng và dễ dàng: - Giao diện web trực quan: Cung cấp giao diện web thân thiện cho phép người dùng xem, tải lên và tải xuống tệp tin một cách dễ dàng, hỗ trợ kéo và thả (drag-and-drop). - Truy cập từ thiết bị di động: Tối ưu hóa hiệu suất để truy cập từ các thiết bị di động như iPad, iPhone và Android. - Hỗ trợ tệp lớn: Cho phép truyền tải các tệp tin có dung lượng lớn (hơn 3GB) và nhiều tệp cùng lúc. - Tiếp tục truyền tải (Resumable Transfers): Nếu quá trình truyền tải bị gián đoạn, người dùng có thể tiếp tục từ điểm dừng thay vì phải bắt đầu lại từ đầu, đặc biệt hữu ích cho các tệp lớn. Quản lý và kiểm soát người dùng: - Quản lý người dùng và nhóm: Dễ dàng tạo, quản lý người dùng và nhóm với các quyền truy cập riêng biệt cho từng thư mục hoặc tệp tin. - Kiểm soát truy cập chi tiết (Granular Control): Cung cấp khả năng kiểm soát chi tiết về băng thông, dung lượng lưu trữ, quyền và truy cập cho từng người dùng, nhóm hoặc miền (domain). - Thư mục ảo (Virtual Folders): Cho phép ánh xạ các thư mục vật lý từ nhiều vị trí khác nhau thành một thư mục ảo trên máy

		chủ FTP, đơn giản hóa cấu trúc thư mục cho người dùng cuối. - Hạn mức và tỷ lệ truyền tải (Transfer Ratio and Quotas): Đặt giới hạn về dung lượng tải lên/tải xuống hoặc tỷ lệ truyền tải cho người dùng để quản lý tài nguyên. - Xác thực người dùng: Tích hợp với Active Directory hoặc LDAP để đơn giản hóa việc xác thực và quản lý người dùng tập trung. Bảo mật: - Mã hóa SSL/TLS: Bảo vệ dữ liệu trong quá trình truyền tải khỏi bị nghe lén, giả mạo hoặc rò rỉ. - Kiểm soát IP: Cho phép chặn hoặc cho phép các địa chỉ IP cụ thể truy cập vào máy chủ để tăng cường bảo mật. - Ngăn chặn tấn công Brute-Force: Có thể cấu hình để tự động chặn các địa chỉ IP có hành vi đăng nhập đáng ngờ (ví dụ: sau nhiều lần đăng nhập sai). - Kiểm soát phiên đồng thời (Concurrent Session Limits): Giới hạn số lượng phiên kết nối đồng thời để quản lý tài nguyên và ngăn chặn lạm dụng. Giám sát và ghi nhật ký: - Ghi nhật ký máy chủ (Server Logs): Ghi lại chi tiết các hoạt động của máy chủ FTP, bao gồm khởi động, cấu hình, tắt máy, các phiên truyền tệp và lỗi để dễ dàng khắc phục sự cố và kiểm tra. - Giám sát phiên thời gian thực: Theo dõi các phiên truyền tệp đang hoạt động và xem thống kê truyền tệp theo thời gian thực. Tự động hóa sự kiện: - Tự động hóa hành động dựa trên sự kiện: Cho phép cấu hình các hành động tự động (ví dụ: gửi email, chạy chương trình, xóa tệp) khi các sự kiện cụ thể xảy ra trên máy chủ (ví dụ: tệp được tải lên, lỗi truyền tải). Dễ dàng quản trị và triển khai:

		- Bảng điều khiển quản lý tập trung: Quản lý tất cả các khía cạnh của máy chủ FTP từ một giao diện quản lý dễ sử dụng. - Hỗ trợ đa hệ điều hành: Có thể triển khai trên cả hệ điều hành Windows và Linux. Thời hạn sử dụng: 3 năm
B	**DỊCH VỤ LIÊN QUAN**	
1	Gia hạn license cho hệ thống lưu trữ hiện hữu Nutanix NX-1175S-G7: Gia hạn dịch vụ bảo hành cho appliance NX-1175S-G7 (thời hạn 2 năm)	Gia hạn dịch vụ bảo hành cho appliance NX-1175S-G7 (đang sử dụng tại Đài). Dịch vụ hỗ trợ: 24/7. Dịch vụ bảo hành trên dùng gia hạn dịch vụ bảo hành cho thiết bị đang hoạt động ở Đài. Chi tiết dịch vụ: - Gia hạn dịch vụ bảo hành cho appliance NX- 1175S-G7 (24/7 Production Level Short Term Support Renewal for Nutanix HCI appliance) - Tính năng: Dịch vụ hỗ trợ phần cứng bao gồm: o Hỗ trợ kỹ thuật 24*7*365 thông qua điện thoại và web support o Cung cấp phần cứng thay thế tại Đài sau khi đã phân tích lỗi Cung cấp kỹ sư hỗ trợ thay thế phần cứng tại Đài sau khi phân tích lỗi (nếu có yêu cầu hỗ trợ từ Đài) Thời hạn sử dụng: 2 năm
2	Gia hạn bảo hành thiết bị phần cứng firewall Checkpoint 6400 hiện hữu (thời hạn 2 năm)	- Dịch vụ support xử lý sự cố kỹ thuật 24x7 - Được bảo hành/ thay thế thiết bị khi hư hỏng phần cứng - Cam kết response time cho các sự cố kỹ thuật: trong vòng 30 phút- 4 giờ tuỳ theo mức độ nghiêm trọng của sự cố. Được cập nhật các bản hot fix, bản nâng cấp và các tính năng mới nhất. Thời hạn sử dụng: 2 năm

- Đối với các mục có yêu cầu cung cấp tài liệu kỹ thuật, trường hợp tài liệu tham chiếu (Các tài liệu và tư liệu bổ trợ trong E-HSDT như Catalog, hồ sơ, giấy tờ, bản vẽ, số liệu…) để chứng minh sự đáp ứng các thông số kỹ thuật của hàng hóa dự thầu kèm trong E-HSDT có thông số kỹ thuật khác với thông số kỹ thuật

do nhà thầu tuyên bố đáp ứng hoặc tài liệu kỹ thuật được công bố rộng rãi trên địa chỉ tham chiếu có thể tải về từ website chính thức của nhà sản xuất, nhà thầu phải cung cấp văn bản xác nhận của nhà sản xuất kèm theo E-HSDT.

3. Các yêu cầu khác

Các yêu cầu khác về kỹ thuật bao gồm yêu cầu về về dịch vụ liên quan như lắp đặt, bảo trì, bảo hành, đào tạo, chuyển giao công nghệ... **Trong E-HSDT, Nhà thầu phải nộp các tài liệu để cam kết, chứng minh đáp ứng tất cả các yêu cầu khác về kỹ thuật dưới đây.**

TT	Các tiêu chí kỹ thuật	Yêu cầu kỹ thuật chi tiết
I	**Yêu cầu về bảo hành, bảo trì**	
1	Thời gian bảo hành	- Thời hạn bảo hành là 2 năm đối với các mục 1, 2, 3, 4, 5, 6, 7, 8, 9 trong phần A bảng Tiêu chuẩn đánh giá về kỹ thuật thuộc chương III, mục 1,2 trong phần B bảng Tiêu chuẩn đánh giá về kỹ thuật thuộc chương III kể từ ngày nghiệm thu đưa vào sử dụng hoặc từ ngày hết hạn bản quyền (license) hiện hữu của HTV (nếu sau ngày ký hợp đồng). - Thời hạn bảo hành là 3 năm đối với mục 10 trong phần A bảng Tiêu chuẩn đánh giá về kỹ thuật thuộc chương III kể từ ngày nghiệm thu đưa vào sử dụng hoặc từ ngày hết hạn bản quyền (license) hiện hữu của HTV (nếu sau ngày ký hợp đồng).
2	Yêu cầu về bảo hành, bảo trì	**** Chính sách bảo hành*** - Bảo hành cho toàn bộ hàng hóa theo tiêu chuẩn của nhà sản xuất - Các hàng hóa do Nhà thầu cung cấp đều được hưởng dịch vụ bảo hành miễn phí: khắc phục các lỗi hệ thống do hàng hóa hỏng hóc, lỗi cài đặt, cấu hình; thực hiện kiểm tra, hiệu chỉnh các hàng hóa của hệ thống trong thời gian bảo hành quy định. - Thời hạn thực hiện bảo hành được tính kể từ ngày ký biên bản nghiệm thu đưa vào sử dụng hoặc từ ngày hết hạn license hiện hữu của HTV (nếu sau ngày ký hợp đồng). **** Nội dung bảo hành***

		- Khắc phục các lỗi phần cứng và phần mềm của hệ thống. - Thực hiện vá lỗi, cập nhật miễn phí các bản vá lỗi của phần mềm hệ thống. - Trong các trường hợp cần thiết trong quá trình vận hành, nhà thầu cần có nhân sự phối hợp hướng dẫn vận hành đối với hệ thống từ xa thông qua điện thoại, email, chat, công cụ hỗ trợ trực tuyến khác (ultraview, teamvier…). - Đối với "mục B dịch vụ liên quan" thuộc bảng Tiêu chuẩn đánh giá về kỹ thuật thuộc chương III, toàn bộ những trường hợp thiết bị hỏng hóc khi vận hành sẽ được nhà thầu thay thế trong thời gian bảo hành và nhà thầu phải hoàn toàn chịu trách nhiệm chi trả các chi phí. - Địa điểm thực hiện: Tại các địa điểm triển khai lắp đặt, cài đặt hàng hóa của chủ đầu tư. - Nhà thầu cung cấp đường dây nóng hỗ trợ kỹ thuật 24/7, cam kết có hỗ trợ kỹ thuật trực tuyến (online) hoặc hỗ trợ kỹ thuật trực tiếp tại địa điểm lắp đặt thiết bị trong thời gian 48 giờ kể từ khi nhận được phát sinh yêu cầu hỗ trợ từ người sử dụng. Đối với các hư hỏng; các lỗi không thể khắc phục và giải quyết tại chỗ: Nhà thầu phải có thông báo kế hoạch giải quyết/ sửa chữa cho chủ đầu tư, đồng thời có phương án/ thiết bị tương đương cho chủ đầu tư sử dụng trong thời gian giải quyết/ sửa chữa. Toàn bộ chi phí khắc phục, giải quyết, sửa chữa do Nhà thầu chi trả.
II	**Yêu cầu về thời gian thực hiện gói thầu** *(bao gồm cung cấp hàng hóa và nghiệm thu),* trong đó	≤ 110 ngày
	Thời gian cung cấp hàng hóa	≤ 40 ngày
III	**Yêu cầu về kết quả thực hiện hợp đồng của nhà thầu theo quy định tại Điều 19 và Điều 20**	

	của Nghị định số 214/2025/NĐ-CP	
1	Uy tín của nhà thầu trong việc tham dự thầu, bao gồm thông tin về các hành vi vi phạm trong quá trình tham dự thầu	Nhà thầu không vi phạm các điều sau đây: a) Nhà thầu không tiến hành hoặc từ chối đối chiếu tài liệu hoặc đã đối chiếu tài liệu nhưng từ chối hoặc không ký biên bản đối chiếu tài liệu trong thời gian có hiệu lực của hồ sơ dự thầu, hồ sơ đề xuất khi được mời đối chiếu tài liệu; b) Nhà thầu không tiến hành hoặc từ chối thương thảo hợp đồng (nếu có) hoặc đã tiến hành nhưng từ chối hoặc không ký kết biên bản thương thảo hợp đồng trong thời gian có hiệu lực của hồ sơ dự thầu, hồ sơ đề xuất khi được mời vào thương thảo hợp đồng, trừ trường hợp quy định tại khoản 7 Điều 45 của Nghị định số 214/2025/NĐ-CP; c) Nhà thầu được lựa chọn trúng thầu nhưng không tiến hành hoặc từ chối tiến hành hoàn thiện hợp đồng, thỏa thuận khung hoặc không ký kết hợp đồng, thỏa thuận khung, trừ trường hợp quy định tại khoản 4 Điều 34 của Nghị định số 214/2025/NĐ-CP; d) Nhà thầu đã ký thỏa thuận khung nhưng không tiến hành hoặc từ chối hoàn thiện hợp đồng hoặc không ký kết hợp đồng. đ) Nhà thầu rút hồ sơ dự thầu, hồ sơ đề xuất sau thời điểm đóng thầu và trong thời gian có hiệu lực của hồ sơ dự thầu, hồ sơ đề xuất; e) Nhà thầu không nộp bản gốc bảo đảm dự thầu theo yêu cầu của chủ đầu tư hoặc không nộp tiền mặt, séc bảo chi, thư bảo lãnh dự thầu hoặc giấy chứng nhận bảo hiểm bảo lãnh theo quy định của pháp luật về đấu thầu; g) Nhà thầu không thực hiện biện pháp bảo đảm thực hiện hợp đồng; h) Nhà thầu từ chối hoặc không xác nhận về việc chấp thuận được trao hợp đồng trong thời gian tối đa 03 ngày làm việc kể từ ngày chủ

		đầu tư mời nhà thầu xác nhận về việc chấp thuận được trao hợp đồng trên Hệ thống mạng đấu thầu quốc gia hoặc đã trúng thầu nhưng không thực hiện theo cam kết trong đơn dự thầu đối với chào giá trực tuyến rút gọn; i) Nhà thầu không bố trí được nhân sự chủ chốt, thiết bị thi công chủ yếu để thực hiện gói thầu xây lắp, PC, phần xây lắp trong gói thầu EC theo cam kết trong đơn dự thầu đối với đấu thầu trong nước. ** Trong E-HSDT, Nhà thầu phải cam kết các nội dung trên, trường hợp cam kết thiếu nội dung, nhà thầu có trách nhiệm làm rõ theo yêu cầu của Chủ đầu tư. Trường hợp, Chủ đầu tư tra cứu trên Hệ thống mạng đấu thầu quốc gia cho thấy nhà thầu có vi phạm các quy định trên thì nhà thầu sẽ bị loại.*
2	Kết quả thực hiện hợp đồng của nhà thầu thông qua việc thực hiện các hợp đồng tương tự trước đó trong thời gian 03 năm gần đây tính đến thời điểm đóng thầu.	Nhà thầu không vi phạm các điều sau đây: - Không có hợp đồng tương tự chậm tiến độ do lỗi nhà thầu, bỏ dở hợp đồng tương tự do lỗi của nhà thầu. - Vi phạm hợp đồng, bị chấm dứt hợp đồng do lỗi của nhà thầu. - Cung cấp hang hóa, dịch vụ không đạt yêu cầu chất lượng theo hợp đồng. ** Trong E-HSDT, Nhà thầu phải cam kết các nội dung trên, trường hợp cam kết thiếu nội dung, nhà thầu có trách nhiệm làm rõ theo yêu cầu của Chủ đầu tư. Trường hợp, Chủ đầu tư tra cứu trên Hệ thống mạng đấu thầu quốc gia cho thấy nhà thầu có vi phạm các quy định trên thì nhà thầu sẽ bị loại.*

3.2. Yêu cầu về bảo hành

Thời gian bảo hành:

- Bảo hành hàng hóa: Thời hạn bảo hành là 2 năm đối với các mục 1, 2, 3, 4, 5, 6, 7, 8, 9 trong phần A bảng Tiêu chuẩn yêu cầu kỹ thuật chương III, mục 1,2 trong phần B bảng Tiêu chuẩn yêu cầu kỹ thuật chương III kể từ ngày nghiệm thu đưa vào sử dụng hoặc từ ngày hết hạn bản quyền (license) hiện hữu của HTV (nếu sau ngày ký hợp đồng).

- Thời hạn bảo hành là 3 năm đối với mục 10 trong phần A bảng Tiêu chuẩn yêu cầu kỹ thuật chương III kể từ ngày nghiệm thu đưa vào sử dụng dụng hoặc từ ngày hết hạn bản quyền (license) hiện hữu của HTV (nếu sau ngày ký hợp đồng).

- Trong thời hạn bảo hành phải bảo đảm khôi phục máy trong vòng 72 giờ từ khi có sự cố xảy ra

- Khuyến khích tăng thời gian bảo hành.

4. Bản vẽ : không áp dụng.

5. Kiểm tra và thử nghiệm:

Chủ đầu tư sẽ kiểm tra khi nhận hàng. Trường hợp hàng hóa không đúng nội dung, chất lượng theo hợp đồng, chủ đầu tư có quyền từ chối nhận hàng.