Phần 2. YÊU CẦU VỀ KỸ THUẬT

Chương V. YÊU CẦU VỀ KỸ THUẬT

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

- Tên gói thầu: Thuê giải pháp đảm bảo an toàn thông tin cho Hệ thống thông tin giải quyết thủ tục hành chính của Bộ KH&CN theo văn bản số 708/BTTTT-CATTT phục vụ kết nối cơ sở dữ liệu quốc gia về dân cư

- Tên dự án, dự toán mua sắm: Dự toán chi tiết một số nhiệm vụ thực hiện năm 2026 thuộc Quyết định số 2037/QĐ-BKHCN ngày 05/8/2025 của Bộ trưởng Bộ Khoa học và Công nghệ giao Phòng Chuyển đổi số nội bộ

- Chủ đầu tư: Trung tâm Công nghệ thông tin;

- Hình thức và phương thức lựa chọn nhà thầu: Chào hàng cạnh tranh

- Thời gian tổ chức lựa chọn nhà thầu: 40 ngày.

- Loại hợp đồng: Trọn gói.

- Thời gian thực hiện gói thầu: 9 tháng, đến 31 tháng 12 năm 2026.

- Phương thức lựa chọn nhà thầu: Một giai đoạn, một túi hồ sơ.

- Nguồn vốn: Chi sự nghiệp khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số (Loại 100 – Khoản 121) giao tại Quyết định số 4558/QĐ-BKHCN ngày 30/12/2025 của Bộ khoa học và Công nghệ.

- Địa điểm thực hiện: Trung tâm Công nghệ thông tin, Tầng 19-20, tòa nhà Cục Viễn thông, đường Dương Đình Nghệ, phường Cầu Giấy, TP Hà Nội.

- Nội dung, quy mô, phạm vi:

+ Nội dung: Thuê giải pháp đảm bảo an toàn thông tin cho Hệ thống thông tin giải quyết thủ tục hành chính của Bộ KH&CN theo văn bản số 708/BTTTT-CATTT phục vụ kết nối cơ sở dữ liệu quốc gia về dân cư.

+ Quy mô: Áp dụng cho Hệ thống thông tin giải quyết thủ tục hành chính của Bộ KH&CN phục vụ kết nối cơ sở dữ liệu quốc gia về dân cư.

+ Phạm vi: Phạm vi, khối lượng các hạng mục thuê dịch vụ công nghệ thông tin bao gồm:

STT	Danh mục dịch vụ	Đơn vị	Số lượng	Ghi chú
1	**VPN Gateway - Palo Alto & IPS/IDS SRX5400:** **(05 máy)** Giải pháp/Thiết bị VPN. Dịch vụ tường lửa đa lớp Tường lửa; hệ thống IDS/IPS.	Tháng	9	

STT	Danh mục dịch vụ	Đơn vị	Số lượng	Ghi chú
	Các thiết bị mạng chính phải được đầu tư theo cặp để dự phòng lẫn nhau			
2	**Dịch vụ Anti DDoS: (01 gói dịch vụ)** Giải pháp giám sát, phát hiện và cảnh báo tấn công AntiDDos - Kênh có tốc độ từ 01-100Mbps - Bao gồm 16 IPv4 và 01 Subnet 56 IPv6	Tháng	9	
3	**DBF Oracle Vault: (01 Gói dịch vụ)** Giải pháp/Thiết bị tường lửa CSDL	Tháng	9	
4	**F5 i7600 ASM: (01 Domain)** Tường lửa ứng dụng Web. Cân bằng tải	Tháng	9	
5	**Hệ thống giám sát Zabbix: (01 Gói dịch vụ)** Giám sát hệ thống thông tin tập trung (Network monitoring).	Tháng	9	
6	**MSS: (500 EPS)** Hệ thống SIEM.	Tháng	9	
7	**Backup tập trung: (1TB)** Hệ thống SAN, SAN Switch	Tháng	9	
8	**Phần mềm chống thất thoát dữ liệu: (01 VM)** Giải pháp DLP	Tháng	9	
9	**Phòng chống mã độc: (01 VM)** Có chức năng Antivirus quản lý tập trung	Tháng	9	
10	**Kiểm thử xâm nhập:** Kiểm tra an toàn thông tin định kỳ (Ứng dụng 1 năm/1 lần)	Gói dịch vụ	1	

Ghi chú:

+ VM: Virtual Machine (Máy ảo) - là môi trường máy tính dựa trên phần mềm hoạt động như một máy tính vật lý độc lập, chạy hệ điều hành và ứng dụng riêng trên tài nguyên phần cứng vay mượn từ máy chủ.

2. Mục tiêu công việc:

2.1. Mục tiêu chung

Đáp ứng đầy đủ các tiêu chí, yêu cầu về an toàn thông tin theo cấp độ, tuân thủ văn bản số 1552/BTTTT-THH và văn bản số 708/BTTTT-CATTT, bảo đảm điều kiện kỹ thuật bắt buộc để thực hiện kết nối Cơ sở dữ liệu quốc gia về dân cư.

Thiết lập hệ thống bảo vệ nhiều lớp (multi-layer security), bao gồm các giải pháp như tường lửa thế hệ mới, WAF, Anti-DDoS, giám sát an toàn thông tin

24/7 (MSS) và các biện pháp kỹ thuật liên quan, nhằm phòng ngừa, phát hiện và xử lý kịp thời các nguy cơ tấn công mạng.

Bảo đảm an toàn, bảo mật và toàn vẹn dữ liệu công dân trong quá trình truyền nhận, khai thác và chia sẻ dữ liệu với Cơ sở dữ liệu quốc gia về dân cư.

Duy trì hoạt động ổn định, liên tục của hệ thống, hạn chế tối đa nguy cơ gián đoạn dịch vụ công trực tuyến do sự cố an toàn thông tin.

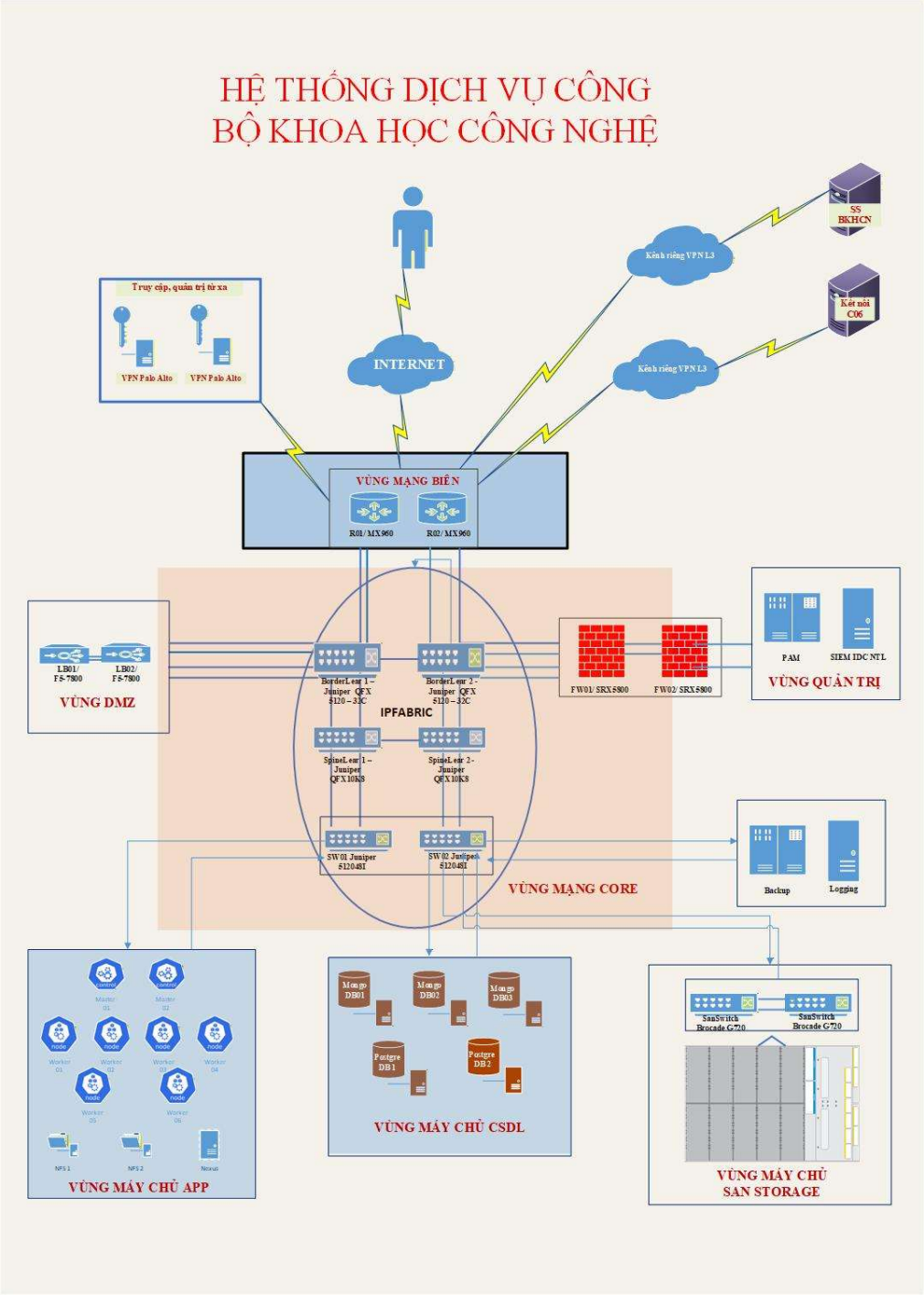
Nâng cao năng lực giám sát, cảnh báo và ứng cứu sự cố an toàn thông tin, giảm thiểu rủi ro pháp lý, kỹ thuật và uy tín trong quá trình vận hành hệ thống.

2.2. Mục tiêu cụ thể

2.2.1 Yêu cầu về chất lượng dịch vụ công nghệ thông tin

Đáp ứng tiêu chuẩn, quy định của Bộ Thông tin và Truyền Thông theo nghị định Nghị định 85/2016/NĐ-CP ngày 01/07/2016 về việc về bảo đảm an toàn hệ thống thông tin theo cấp độ, và các nội dung hướng dẫn của Thông tư 12/2022/TT-BTTTT ngày 12/08/2022 về việc quy định chi tiết và hướng dẫn một số điều của nghị định số 85/2016/nđ-cp ngày 01/7/2016 của chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

Đáp ứng mô hình hạ tầng quản lý và vận hành Hệ thống giải quyết thủ tục hành chính của Bộ KH&CN.



Các nội dung yêu cầu về chất lượng dịch vụ công nghệ thông tin cụ thể như sau:

- Đáp ứng đầy đủ các tiêu chí, yêu cầu về an toàn thông tin theo cấp độ, tuân thủ văn bản số 1552/BTTTT-THH và văn bản số 708/BTTTT-CATTT, bảo đảm điều kiện kỹ thuật bắt buộc để thực hiện kết nối Cơ sở dữ liệu quốc gia về dân cư.

- Thiết lập hệ thống bảo vệ nhiều lớp (multi-layer security), bao gồm các giải pháp như tường lửa thế hệ mới, WAF, Anti-DDoS, giám sát an toàn thông tin 24/7 và các biện pháp kỹ thuật liên quan, nhằm phòng ngừa, phát hiện và xử lý kịp thời các nguy cơ tấn công mạng.
- Bảo đảm an toàn, bảo mật và toàn vẹn dữ liệu công dân trong quá trình truyền nhận, khai thác và chia sẻ dữ liệu với Cơ sở dữ liệu quốc gia về dân cư.
- Duy trì hoạt động ổn định, liên tục của hệ thống, hạn chế tối đa nguy cơ gián đoạn dịch vụ công trực tuyến do sự cố an toàn thông tin.
- Nâng cao năng lực giám sát, cảnh báo và ứng cứu sự cố an toàn thông tin, giảm thiểu rủi ro pháp lý, kỹ thuật và uy tín trong quá trình vận hành hệ thống.

2.2.2 Yêu cầu về kỹ thuật, công nghệ

Yêu cầu danh mục quy chuẩn, tiêu chuẩn kỹ thuật cần áp dụng

+ Nghị định 85/2016/NĐ-CP ngày 01/7/2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ;

+ Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

+ Tiêu chuẩn quốc gia TCVN 11930:2017 về Công nghệ thông tin - các kỹ thuật an toàn - yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ.

2.2.3. Yêu cầu về quản trị, vận hành, bảo trì dịch vụ

Việc quản trị, vận hành, bảo trì dịch vụ phải do nhà cung cấp dịch vụ thực hiện, và phải được bao gồm trong gói dịch vụ được thuê.

Đơn vị cung cấp dịch vụ phải phối hợp với bên thuê để tổ chức quản trị, vận hành, giám sát. Trong quá trình thuê đơn vị thuê phải có:

- Báo cáo sự cố.
- Báo cáo xử lý yêu cầu hỗ trợ.
- Báo cáo đánh giá, tối ưu hệ thống (hiện trạng sử dụng, vấn đề, khuyến nghị, tối ưu).

2.2.4. Yêu cầu hướng dẫn sử dụng

+ Có quy trình xử lý sự cố, sơ đồ và mô tả từng bước của quy trình xử lý sự cố.

2.2.5. Các cam kết về an toàn thông tin mạng, bảo vệ thông tin người sử dụng trong và sau khi kết thúc hợp đồng thuê dịch vụ CNTT

Nhà cung cấp dịch vụ CNTT phải cam kết bảo mật các thông tin về hệ thống triển khai trong và sau khi kết thúc hợp đồng cung cấp dịch vụ CNTT bằng cách tuân thủ quy định (bảo mật) dữ liệu thông tin cá nhân, và tất cả các văn bản pháp luật có liên quan, đồng thời đảm bảo sự tuân thủ của đội ngũ nhân viên với các

chuẩn mực nghiêm ngặt về sự an toàn và tính bảo mật. bao gồm những nội dung như sau:

- Không được phép sao chép, cung cấp một phần hay toàn bộ thông tin bảo mật cho bất kỳ bên thứ ba nào biết khi chưa có sự chấp thuận bằng văn bản của bên có quyền sở hữu đối với thông tin bảo mật.

- Không được sử dụng thông tin bảo mật mà các bên đã cung cấp cho nhau phục vụ cho các mục đích khác ngoài nội dung kế hoạch thuê hai bên thực hiện.

- Cam kết bảo đảm không tiết lộ thông tin bảo mật cho bất kỳ bên thứ ba nào khác, trừ khi có yêu cầu của cơ quan chức năng hoặc được sự chấp thuận bằng văn bản của cả hai bên.

2.2.6. Các yêu cầu phi chức năng khác

(1) Tính sẵn sàng

Đối với các hệ thống bảo vệ ATTT trực tiếp thời gian chết (downtime) có thể dẫn đến rủi ro. Tính sẵn sàng cao hỗ trợ đảm bảo hệ thống hoạt động 24/7.

(2) Hiệu năng và khả năng xử lý

Dịch vụ phải xử lý lưu lượng truy cập của hệ thống mà không làm suy giảm hiệu năng hệ thống ứng dụng. Hệ thống bảo mật phải có khả năng mở rộng khi lưu lượng tăng. Không làm tăng độ trễ truy cập quá mức cho phép.

(3) Yêu cầu về kiểm thử và đánh giá an toàn

Hệ thống phải được kiểm thử xâm nhập định kỳ theo các tiêu chuẩn như OWASP Testing Guide.Thực hiện đánh giá lỗ hổng bảo mật định kỳ hằng năm

3. Yêu cầu kỹ thuật của gói thầu:

- Nhà thầu trình bày chi tiết các công việc cho từng phần riêng biệt đảm bảo các danh mục dịch vụ đều đạt được yêu cầu đầu ra.

STT	Danh mục dịch vụ	Yêu cầu về đầu ra
1	**VPN Gateway - Palo Alto & IPS/IDS SRX5400: (05 máy)** Giải pháp/Thiết bị VPN. Dịch vụ tường lửa đa lớp Tường lửa; hệ thống IDS/IPS. Các thiết bị mạng chính phải được đầu tư theo cặp để dự phòng lẫn nhau.	- Dịch vụ cung cấp: **+ IPsec (Internet Protocol Security):** Cung cấp bảo mật ở mức mạng, với các cơ chế mã hóa và xác thực dữ liệu. **+ SSL (Secure Sockets Layer):** giúp thiết lập kênh mã hóa an toàn qua HTTPS. - Dữ liệu truyền qua kênh VPN được mã hóa, ngăn chặn nghe lén, đánh cắp dữ liệu. - Giảm nguy cơ bị tấn công khi làm việc qua Wi-Fi công cộng. - Hỗ trợ quản trị an toàn từ xa: triển khai cho nhân viên từ xa mà không cần cài đặt phức tạp, quản trị viên có thể quản lý quyền truy cập theo vai trò, người dùng hoặc thiết bị.

STT	Danh mục dịch vụ	Yêu cầu về đầu ra
2	**Dịch vụ Anti DDoS: (01 gói dịch vụ)** Giải pháp giám sát, phát hiện và cảnh báo tấn công AntiDDos - Kênh có tốc độ từ 01-100Mbps - Bao gồm 16 IPv4 và 01 Subnet 56 IPv6	- Ngăn chặn và giảm thiểu tác động, bảo đảm rằng dịch vụ và tài nguyên hệ thống vẫn hoạt động bình thường trong điều kiện tấn công. - Giám sát, phát hiện & cảnh báo tấn công. - Giám sát & phân tích lưu lượng dịch vụ. - Chặn lưu lượng theo thông tin đặc tả lưu lượng - Điều hướng & làm sạch lưu lượng tấn công
3	**DBF Oracle Vault: (01 Gói dịch vụ)** Giải pháp/Thiết bị tường lửa CSDL	Cung cấp tường lửa chuyên dụng giúp bảo vệ ở cấp độ giao tiếp giữa người dùng/ứng dụng và cơ sở dữ liệu, các tính năng: - Bảo vệ trước các tấn công SQL Injection: Phát hiện và ngăn chặn các truy vấn SQL độc hại trước khi chúng xâm nhập vào cơ sở dữ liệu. - Tăng cường bảo mật dữ liệu: Bảo vệ thông tin nhạy cảm, ngăn chặn truy cập không được phép từ cả bên trong và bên ngoài tổ chức. - Đảm bảo tuân thủ pháp lý: Hỗ trợ các tiêu chuẩn bảo mật như GDPR, PCI DSS, HIPAA, ISO 27001. - Giám sát và ghi nhật ký:Theo dõi toàn bộ hoạt động truy cập cơ sở dữ liệu và cung cấp báo cáo chi tiết phục vụ kiểm tra an ninh. - Ngăn chặn truy vấn bất thường: Tự động phát hiện và chặn các lệnh SQL vượt quá phạm vi truy cập của người dùng hoặc ứng dụng. - Hỗ trợ phân quyền: Kiểm soát quyền truy cập dựa trên vai trò hoặc chính sách tổ chức.
4	**F5 i7600 ASM: (01 Domain)** Tường lửa ứng dụng Web. Cân bằng tải	Cung cấp tường lửa ứng dụng web để bảo vệ các ứng dụng web khỏi các cuộc tấn công như SQL Injection, Cross-Site Scripting (XSS), File Inclusion, và DDoS **Các tính năng cao cấp như:** - Phân tích mẫu chữ ký (Signature-based Detection): Dựa trên các mẫu tấn công đã biết, WAF so sánh lưu lượng truy cập với cơ sở dữ liệu để phát hiện các mối đe dọa. - Phân tích hành vi bất thường (Anomaly-based Detection): Xác định các yêu cầu bất thường không phù hợp với hành vi bình thường của ứng dụng. - Chính sách bảo mật tùy chỉnh (Custom Rules): Quản trị viên có thể thiết lập các quy tắc đặc thù dựa trên nhu cầu bảo mật của tổ chức.

STT	Danh mục dịch vụ	Yêu cầu về đầu ra
		- Kiểm tra ngữ nghĩa (Semantic Analysis): Đánh giá ý nghĩa của các yêu cầu HTTP/HTTPS để phát hiện tấn công nâng cao như Zero-Day Exploits.
5	**Hệ thống giám sát Zabbix: (01 Gói dịch vụ)** Giám sát hệ thống thông tin tập trung (Network monitoring).	Cung cấp dịch vụ phát hiện và xử lý kịp thời các vấn đề, tối ưu hóa hiệu suất, và đảm bảo máy chủ hoạt động ổn định, đáp ứng yêu cầu của ứng dụng và người dung. Hệ thống giám sát chất lượng dịch vụ phải có tính năng giám sát toàn diện các phương diện sau: Máy chủ ảo hóa (Cloud), Máy chủ (Server), Thời gian hoạt động (Uptime), Gói dữ liệu (Package), cổng (Port), Sử dụng bộ nhớ (Memory Usage), Dịch vụ web (Web Service), Sử dụng ổ đĩa (Disk Usage), Giám sát theo thời gian thực.
6	**MSS: (500 EPS)** Hệ thống SIEM.	- Cung cấp báo cáo Giám sát định kỳ hàng tháng - Cung cấp báo cáo Giám sát cuối kỳ - Tỉ lệ cảnh báo sai/false positive ≤ *20*% - Thời gian tiếp nhận xử lý đối với cảnh báo Nghiêm trọng: ≤ 1 giờ - Thời gian tiếp nhận xử lý đối với cảnh báo Cao: ≤ *24* giờ - Thời gian tiếp nhận xử lý đối với cảnh báo Trung bình: ≤ 72 giờ
7	**Backup tập trung: (1TB)** Hệ thống SAN, SAN Switch	Nhân bản một phần hoặc toàn bộ hệ thống máy chủ lên hạ tầng <u>điện toán đám mây</u>, đảm bảo dự phòng cho việc vận hành khi hệ thống chính gặp lỗi hoặc những sự cố không mong muốn. Yêu cầu: - Backup dữ liệu nhiều hệ điều hành: các hệ điều hành họ Windows, Linux, MacOS - Hỗ trợ sao lưu dữ liệu ứng dụng: Active Directory, MSSQL, Oracle Databases,… - Cơ chế backup tự động theo lịch trình thiết lập sẵn. Backup full, backup incremental -Có khả năng khôi phục lại dữ liệu máy ảo, máy vật lý từ các bản backup; hỗ trợ khôi phục dữ liệu đa cấp độ: file, thư mục, ứng dụng,… - Dữ liệu sao lưu được đảm bảo an toàn trong quá trình sao lưu thông qua kênh truyền mã hóa - Có giao diện quản trị tập trung - Có khả năng nén dữ liệu sao lưu để giảm dung lượng lưu trữ - Có thể mở rộng dung lượng lưu trữ theo yêu cầu của Bộ.

STT	Danh mục dịch vụ	Yêu cầu về đầu ra
8	**Phần mềm chống thất thoát dữ liệu: (01 VM)** Giải pháp DLP	Đối với hệ thống thông tin cấp độ 3 có xử lý thông tin bí mật nhà nước hoặc hệ thống thông tin quy định tại điểm c khoản 2 Điều 9 Nghị định 85/2016/NĐ-CP. Yêu cầu sử dụng Sản phẩm Phòng, chống thất thoát dữ liệu. Bảo đảm tối thiểu các máy chủ cơ sở dữ liệu, máy tính quản trị cơ sở dữ liệu, máy tính phục vụ hoạt động nghiệp vụ xử lý dữ liệu được triển khai các giải pháp phòng, chống thất thoát dữ liệu. 2. Đối với các hệ thống thông tin cấp độ 3 không yêu cầu bắt buộc sử dụng Sản phẩm Phòng, chống thất thoát dữ liệu thì có phương án đáp ứng các yêu cầu tối thiểu sau: - Sử dụng chức năng phòng, chống thất thoát dữ liệu được tích hợp trên thiết bị/sản phẩm bảo mật sử dụng trong hệ thống (nếu có). - Có tài liệu minh chứng và kiểm tra trực tiếp trên hệ thống việc thiết lập cấu hình tường lửa Hệ điều hành máy chủ cơ sở dữ liệu để quản lý truy cập giữa các máy chủ trong cùng một vùng mạng. - Có tài liệu minh chứng và kiểm tra trực tiếp trên hệ thống việc thực hiện cấu hình tăng cường bảo mật cho Hệ điều hành và Cơ sở dữ liệu. - Có tài liệu minh chứng và kiểm tra trực tiếp trên hệ thống việc thực hiện cấu hình tăng cường bảo mật cho các máy tính quản trị cơ sở dữ liệu, máy tính phục vụ hoạt động nghiệp vụ xử lý dữ liệu.
9	**Phòng chống mã độc: (01 VM)** Có chức năng Antivirus quản lý tập trung	- Đáp ứng chỉ thị số 14/CT-TTg ngày 25/05/2018 của Thủ tướng Chính phủ v/v nâng cao năng lực phòng, chống phần mềm độc hại; - Có chức năng kết nối, chia sẻ thông tin từ hệ thống quản lý tập trung với hệ thống kỹ thuật của cơ quan chức năng theo tiêu chuẩn, quy chuẩn quốc gia và yêu cầu kỹ thuật tại Văn bản số 2290/BTTTT-CATTT ngày 17/7/2018 của Bộ Thông tin và Truyền thông V/v hướng dẫn kết nối, chia sẻ thông tin về mà độc giữa các hệ thống kỹ thuật.
10	**Kiểm thử xâm nhập:** Kiểm tra an toàn thông tin định kỳ (Ứng dụng 1 năm/1 lần)	- Cung cấp báo cáo kiểm thử chi tiết các lỗ hổng và khuyến nghị phương án xử lý cho từng lỗ hổng - Hỗ trợ khách hàng xử lý các lỗ hổng tìm được - Sau 02 tháng triển khai dự án, các bên sẽ thống nhất thời điểm bắt đầu kiểm thử. Thời gian kiểm thử kéo dài tối đa 1 tháng - Đáp ứng tiêu chuẩn OWASP Top 10

4. Giải pháp và phương pháp luận:

Nhà thầu chuẩn bị đề xuất giải pháp, phương pháp luận tổng quát thực hiện dịch vụ theo các nội dung quy định tại Chương này, gồm các phần như sau:

1. Giải pháp và phương pháp luận *[Mô tả hiểu biết về mục tiêu của công việc ghi trong Điều khoản tham chiếu, cách tiếp cận kỹ thuật và phương pháp luận sẽ áp dụng để thực hiện công việc nhằm đạt được kết quả dự kiến và mức độ chi tiết của kết quả đó. Nhà thầu lưu ý không sao chép, nhắc lại Điều khoản tham chiếu trong phần này];*

2. Kế hoạch công tác: *[Kế hoạch thực hiện phải thống nhất với cách tiếp cận kỹ thuật và phương pháp luận, thể hiện sự hiểu biết về Điều khoản tham chiếu và khả năng chuyển Điều khoản tham chiếu thành kế hoạch thực hiện khả thi. Kế hoạch thực hiện phải thống nhất với Kế hoạch tiến độ]*.

5. Quy định về kiểm tra, nghiệm thu sản phẩm:

Căn cứ theo Thông tư số 16/2024/TT-BTTTT ngày 30/12/2024 của Bộ Thông tin và Truyền thông Quy định chi tiết nội dung công tác triển khai, giám sát công tác triển khai, nghiệm thu đối với dự án đầu tư ứng dụng công nghệ thông tin. Theo đó, đối với phần mềm thương mại, phần mềm phổ biến nhà thầu triển khai chủ trì, phối hợp với chủ đầu tư tổ chức vận hành thử.

Nội dung vận hành thử theo hướng dẫn tại Phụ lục số 1 của Phụ lục II ban hành kèm theo Thông tư số 16/2024/TT-BTTTT ngày 30/12/2024 của Bộ Thông tin và Truyền thông. Kết quả vận hành thử được nhà thầu triển khai lập thành báo cáo.

Sản phẩm hoặc hạng mục công việc được hoàn thành đầy đủ về khối lượng, chất lượng, tiến độ, các yêu cầu theo hợp đồng và thiết kế chi tiết được phê duyệt; Chủ đầu tư và các đơn vị có liên quan sẽ thỏa thuận về nội dung nghiệm thu, thời điểm, địa điểm nghiệm thu.

+ Báo cáo kết quả kiểm thử, vận hành thử: 03 bản gốc.

+ Biên bản nghiệm thu công việc cho các hạng mục dịch vụ: 03 bản gốc

+ Biên bản nghiệm thu hoàn thành dịch vụ: 03 bản gốc