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 dự án: Thuê hệ thống giám sát an ninh thông tin SOC.

- Tên gói thầu: Thuê hệ thống giám sát an ninh thông tin SOC.

- Nguồn vốn: Vốn hoạt động kinh doanh của VCBS.

- Giá gói thầu: 4.794.000.000 đồng, đã bao gồm thuế, phí và toàn bộ chi phí khác liên quan (*Bằng chữ: Bốn tỷ, bảy trăm chín mươi bốn triệu đồng.).*

- Hình thức, phương thức lựa chọn nhà thầu: Chào hàng cạnh tranh, trong nước, qua mạng, một giai đoạn một túi hồ sơ.

- Thời gian bắt đầu tổ chức lựa chọn nhà thầu: Quý III năm 2025.

- Loại hợp đồng: Trọn gói.

- Thời gian thực hiện gói thầu: 17 tháng kể từ ngày hợp đồng có hiệu lực, trong đó:

+ Thời gian triển khai hệ thống: 05 tháng kể từ ngày hợp đồng có hiệu lực.

+ Thời gian thuê dịch vụ: 01 năm (12 tháng) Tính từ ngày nghiệm thu hoàn thành việc triển khai và cài đặt hệ thống giám sát ANTT cho hệ thống CNTT của VCBS).

2. Mục tiêu công việc:

a) Định hướng tiêu chuẩn và khung kiến trúc

Để đáp ứng yêu cầu tuân thủ quy định pháp luật về an toàn thông tin, đồng thời đảm bảo hệ thống giao dịch trực tuyến cung cấp cho khách hàng, VCBS xác định định hướng tiêu chuẩn và khung kiến trúc an toàn thông tin như sau:

- Nghị định 85/2016/NĐ-CP Thông tư số 12/2022/TT-BTTTT của Bộ Thông tin và Truyền thông: Đây là yêu cầu bắt buộc VCBS phải tuân thủ theo quy định. Các quy định trong nghị định này yêu cầu tổ chức cần phân loại hệ thống thông tin theo cấp độ và phải triển khai các biện pháp bảo đảm an toàn theo các cấp độ, bao gồm khả năng giám sát, phát hiện và ứng phó sự cố an toàn thông tin 24/7. Các hệ thống thông tin của VCBS chỉ thuộc cấp độ 2 và 3, không thuộc cấp độ 1, cấp độ 4 và cấp độ 5 do không thuộc phạm vi áp dụng, cụ thể như sau:

    - Tiêu chí phân loại với hệ thống cấp độ 2: Theo khoản 1 và khoản 2c Điều 8 Nghị định 85/2016/NĐ-CP, các hệ thống thông tin phục vụ hoạt động nội bộ của cơ quan, tổ chức và có xử lý thông tin riêng, thông tin cá nhân của người sử dụng nhưng không xử lý thông tin bí mật nhà nước và/hoặc cung cấp dịch vụ trực tuyến khác có xử lý thông tin riêng, thông tin cá nhân của dưới 10.000 người sử dụng.

    - Tiêu chí phân loại với hệ thống cấp độ 3: Theo khoản 2b, 2c Điều 9 Nghị

định 85/2016/NĐ-CP, các hệ thống cung cấp dịch vụ trực tuyến thuộc danh mục dịch vụ kinh doanh có điều kiện và/hoặc xử lý thông tin cá nhân của từ 10.000 người trở lên.

- Khung an ninh mạng của Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ (NIST Cybersecurity Framework - NIST CSF): NIST CSF đưa ra cấu trúc quản lý rủi ro an ninh mạng theo 5 chức năng cốt lõi: Nhận diện (Identify), Bảo vệ (Protect), Phát hiện (Detect), Ứng phó (Respond), và Phục hồi (Recover).
- Tiêu chuẩn quốc tế ISO/IEC 27001:2022 về Hệ thống quản lý an toàn thông tin (ISMS): ISO 27001 yêu cầu tổ chức xây dựng, duy trì cơ chế kiểm soát và giám sát an toàn thông tin để bảo vệ tài sản thông tin trước các mối đe dọa ngày càng gia tăng.

b) Mục tiêu mong muốn tối thiểu đối với hệ thống Giám sát an ninh thông tin (SOC)

Dựa trên định hướng khung kiến trúc an toàn thông tin và các tiêu chuẩn, quy định pháp lý đã nêu tại mục a, VCBS mong muốn triển khai Hệ thống giám sát an ninh thông tin (SOC) với các mục tiêu tối thiểu sau:

- Đáp ứng yêu cầu tuân thủ quy định pháp luật Việt Nam và chuẩn hóa hệ thống theo tiêu chuẩn quốc tế:
  - Theo quy định tại Nghị định 85/2016/NĐ-CP và hướng dẫn tại Thông tư 12/2022/TT-BTTTT, hệ thống thông tin cấp độ 3 bắt buộc phải có năng lực giám sát, phát hiện, cảnh báo và ứng phó sự cố an toàn thông tin liên tục 24/7. Việc thiết lập SOC là giải pháp kỹ thuật chủ đạo để đảm bảo thực hiện đầy đủ các yêu cầu này.
  - Theo NIST Cybersecurity Framework (NIST CSF): trong 5 chức năng cốt lõi của NIST (gồm Nhận diện, Bảo vệ, Phát hiện, Ứng phó, và Phục hồi), SOC đảm nhận vai trò triển khai các chức năng Phát hiện (Detect) và Ứng phó (Respond) đối với sự cố an toàn thông tin, đồng thời hỗ trợ chức năng Phục hồi (Recover) sau sự cố.
  - Theo ISO/IEC 27001:2022: SOC đóng vai trò là thành phần trung tâm trong việc kiểm soát, giám sát sự kiện an toàn thông tin, quản lý sự cố, thực hiện các hành động khắc phục và cải tiến liên tục trong hệ thống quản lý an toàn thông tin (ISMS).
- Bảo vệ tài sản thông tin và dữ liệu giao dịch của khách hàng: Hệ thống giao dịch trực tuyến của VCBS xử lý khối lượng lớn thông tin cá nhân, tài chính của khách hàng. Việc xây dựng SOC giúp phát hiện kịp thời các hành vi tấn công, rò rỉ dữ liệu hoặc sự cố an toàn thông tin, giảm thiểu tối đa rủi ro gây tổn thất cho khách hàng và uy tín của công ty.

- Nâng cao năng lực vận hành an toàn hệ thống CNTT tổng thể: Trung tâm SOC không chỉ giám sát riêng các hệ thống giao dịch mà còn mở rộng năng lực giám sát toàn bộ hạ tầng CNTT nội bộ, qua đó tạo nền tảng vận hành ổn định, an toàn và sẵn sàng đáp ứng các yêu cầu phát triển trong tương lai.
- Phù hợp với lộ trình xây dựng kiến trúc an toàn thông tin tổng thể: Theo khung kiến trúc an toàn thông tin VCBS đã định hướng, SOC là một cấu phần quan trọng giúp hiện thực hóa các lớp bảo vệ (multi-layered defense) cho toàn bộ hạ tầng công nghệ thông tin.

3. Yêu cầu kỹ thuật của gói thầu:

a) Yêu cầu về dịch vụ

Hệ thống cung cấp phải có sẵn các tính năng sẵn sàng sử dụng (không phát sinh thêm chi phí) đáp ứng các yêu cầu dưới đây:

STT	Yêu cầu	Mô tả
I	**Yêu cầu chung của dịch vụ**	
1	Yêu cầu hiệu năng	Khả năng đáp ứng thu thập và xử lý dữ liệu tối thiểu 7900 EPS (Event Per Second) hoặc 135 GB/day.
		Có cơ chế buffer để xử lý dữ liệu khi vượt quá license trong một khoảng thời gian xác định.
2	Yêu cầu về hệ thống	• Số lượng thiết bị xử lý và lưu trữ dữ liệu: >= 02 thiết bị. • Đảm bảo tất cả các cấu phần trong hệ thống giám sát an ninh thông tin phải được chạy ở chế độ active-active hoặc active-standby. • Các cấu phần của hệ thống giám sát (bao gồm phần cứng xử lý và lưu trữ, phần mềm xử lý giám sát) phải được đặt tại DC của VCBS. • Hệ thống phải đáp ứng yêu cầu về phân tích và lưu trữ dữ liệu tối thiểu 03 tháng (đối với dữ liệu online) và 09 tháng (đối với dữ liệu offline).
3	Yêu cầu về dịch vụ triển khai, cài đặt	• Triển khai tất cả các cấu phần của hệ thống giám sát an ninh SIEM. • Triển khai tích hợp các nguồn dữ liệu phục vụ giám sát.

		• Thực hiện thu thập, chuẩn hóa và hướng dẫn tối ưu dữ liệu đã thu thập về hệ thống SIEM. • Thực hiện thiết lập các cảnh báo hệ thống bao gồm các cảnh báo theo tập luật và cảnh báo các sự kiện bất thường (Behavior Analytics). • Thực hiện tối ưu các tập luật (rule) khi có các dữ liệu logs mới phát sinh trong hệ thống CNTT của VCBS. • Triển khai các kịch bản (Use Case) giám sát dựa trên thông tin từ các giải pháp trong hạ tầng bảo mật của VCBS. • Triển khai xây dựng dashboard giám sát theo kịch bản SOC. • Xây dựng Portal hệ thống giám sát an ninh thông tin cho Khách hàng. • Thiết lập cơ chế kiểm soát truy cập đa yếu tố (MFA) đối với hệ thống SIEM.
4	Yêu cầu về dịch vụ giám sát ANTT	• Cung cấp nhân sự giám sát an ninh thông tin 24/7 L1, L2&L3. • Giám sát ANTT, phân loại, phân tích, điều tra cảnh báo và ứng cứu, phối hợp xử lý sự cố ANTT trong toàn thời gian cung cấp dịch vụ. • Thực hiện báo cáo định kỳ theo tuần, tháng, quý về tình hình giám sát và xử lý sự cố. • Báo cáo phân tích và xử lý sự cố đối với các sự cố ở mức nghiêm trọng. • Cung cấp hệ thống Workflow/Case Management (Ticket management) để quản lý các sự kiện an ninh bất thường/tấn công được định danh.
5	Yêu cầu về dịch vụ tình báo số (Threat Intelligent)	Cung cấp thông tin tình báo cho hệ thống giám sát an ninh thông tin để kịp thời rà soát điểu yếu, lỗ hổng an ninh và phát hiện sớm các thông tin bị lộ lọt.
6	Giải pháp phần mềm	Giải pháp nằm trong danh sách các Leaders theo đánh giá của Gartner về giải pháp thu thập, giám sát và phân tích log trong 3 năm gần nhất tại đường dẫn: https://www.gartner.com/doc/reprints?id=1-2HIOXQSL&ct=240509&st=sb
7	Bản quyền mềm	Bản quyền cho toàn bộ các tính năng phần mềm của hệ thống SIEM ở phụ lục này phải là bản quyền thương mại.

		Trong trường hợp phần mềm đứng tên nhà cung cấp, nhà cung cấp dịch vụ phải cung cấp đầy đủ giấy tờ chứng minh rằng "*phần mềm được cấp phép bởi các hãng sản xuất để cung cấp dịch vụ cho riêng VCBS"*.
II	**Yêu cầu bản quyền phần hệ thống SIEM**	
1	Yêu cầu về mô hình triển khai.	Hệ thống triển khai theo kiến trúc tập trung hoặc phân tán có các thành phần phân tích tại site chính và site dự phòng.
		Hệ thống có tính năng cấu hình để kiểm soát tốc độ xử lý trong quá trình thu thập sự kiện.
2	Yêu cầu về quản trị hệ thống.	Quản trị thông qua tối thiểu gồm: CLI, Web GUI.
		Hệ thống có chức năng phân quyền người dùng hệ thống theo vai trò (Role-based access control).
3	Khả năng thu thập và chuẩn hóa dữ liệu của hệ thống.	Có khả năng thu thập dữ liệu từ nhiều nguồn dữ liệu khác nhau, tối thiểu bao gồm: - Logs các máy chủ - Logs các ứng dụng - Logs các thiết bị mạng và bảo mật.
		Có khả năng thu thập dữ liệu không cần phân biệt dữ liệu có cấu trúc hay không có cấu trúc.
		Có khả năng thu thập các dữ liệu mới được sinh ra theo thời gian thực.
		Có khả năng xây dựng index của dữ liệu mà không cần tuân theo lược đồ dữ liệu đầu vào.
		Có khả năng che các thông tin nhạy cảm (masking) trong dữ liệu raw trước khi hiển thị lên dashboard, đảm bảo tính bí mật của thông tin (như thông tin tài khoản người dùng, thông tin mật khẩu,…)
		Dữ liệu đã thu thập yêu cầu đảm bảo có bản lưu dữ liệu nguyên gốc (raw - chưa xử lý), có thể trích xuất dữ liệu raw nguyên gốc bất cứ khi nào cần.
4	Khả năng tìm kiếm và phân	Có khả năng tìm kiếm cùng lúc trên nhiều nguồn dữ liệu, nhiều định dạng khác nhau để xâu chuỗi các thông tin liên quan.

	tích dữ liệu của hệ thống.	Cung cấp công cụ tự động và thủ công trên giao diện web để phân tách các trường thông tin để hiểu rõ hơn về ý nghĩa của các dữ liệu log, thuận tiện cho đội ngũ quản trị sử dụng.
		Cho phép tự động phát hiện các sự kiện bất thường hoặc dữ liệu ngoại lệ thông qua các mẫu dữ liệu lịch sử.
		Cung cấp bộ luật detection rules sẵn có theo khung MITRE ATT&ACK
		Cho phép phân tích tương quan sự kiện (Correlation Analysis) theo các quy tắc: bất thường (anomaly), theo hành vi (behavior), và theo ngưỡng (threshold).
5	Khả năng bổ sung tri thức để làm giàu dữ liệu của hệ thống.	Có khả năng cho phép hệ thống và người dùng tự động thêm các nguồn tri thức để làm giàu dữ liệu.
		Có khả năng cho phép xác định và phân loại các giao dịch bằng cách tương quan sự kiện trên nhiều nguồn dữ liệu khác nhau.
		Có khả năng chia sẻ các câu lệnh tìm kiếm, các báo cáo cho các người dùng khác nhau trong hệ thống.
		Có khả năng tích hợp với các nguồn tri thức Threat intelligent để cập nhật các mẫu tấn công, rủi ro mới nhất theo chuẩn mở STIX/TAXII.
		Có khả năng quản lý hành vi người dùng User Behavior Analytics để giám sát các rủi ro từ bên trong.
6	Khả năng giám sát, cảnh báo của hệ thống.	Có khả năng thiết lập các điều kiện cảnh báo dựa trên các ngưỡng do người dùng quy định trước.
		Có khả năng cho phép theo dõi và tự động khắc phục sự cố thông qua các script hoặc Web Hook.
7	Khả năng phân tích và báo cáo của hệ thống.	Có khả năng hỗ trợ phân tích, thống kê bằng cách kết hợp các câu lệnh tìm kiếm nâng cao trong một câu lệnh tìm kiếm.
		Cho phép cài đặt/tùy chỉnh để có chức năng tùy biến báo cáo theo các dạng khác nhau: time-base charts, bar, pie.
		Có khả năng trích xuất báo cáo ở dạng PDF theo yêu cầu hoặc lập lịch.

8	Khả năng tạo và tùy chỉnh Dashboard của hệ thống.	Có khả năng tạo và chỉnh sửa dashboard bằng cách kết hợp các kết quả tìm kiếm, báo cáo, bảng và biểu đồ.
		Có sẵn tính năng tích hợp với các ứng dụng phổ biến của bên thứ ba như: Solarwind, Dynatrace hoặc các hệ thống syslog khác.
		Có khả năng kéo thả các panel trên dashboard, sắp xếp vị trí tùy ý theo nhu cầu của người sử dụng.
9	Khả năng xây dựng và phát triển ứng dụng của hệ thống.	Có khả năng thu thập và phân tích log được đẩy về từ hệ thống khác hoặc chủ động lấy log bằng cách gọi tới API của các hệ thống khác và phân tích log lấy về.
		Cho phép tùy biến giao diện với tối thiểu ngôn ngữ tiếng Anh hoặc tiếng Việt.
10	Triển khai và mở rộng của hệ thống.	Cho phép hỗ trợ triển khai và mở rộng hệ thống trên tối thiểu các hệ điều hành Linux hoặc Windows.
		Có khả năng giám sát để phát hiện các thay đổi cấu hình trái phép trên chính hệ thống SIEM.
11	Yêu cầu về bảo mật của hệ thống.	Cho phép cấu hình hạn chế truy cập vào các nguồn dữ liệu, loại dữ liệu, khoảng thời gian, xem, báo cáo hoặc dashboard cụ thể.
		Hệ thống có khả năng xác thực người dùng thông qua LDAP và có khả năng xác thực hai yếu tố bằng cách tích hợp với giải pháp khác.
		Có khả năng cho phép người dùng truy cập an toàn thông qua giao thức HTTPS.
		Cho phép xác nhận tính toàn vẹn của dữ liệu index theo nhu cầu để đảm bảo tính an toàn và tuân thủ.
12	Khả năng giám sát bảo mật tổng thể của hệ thống.	Tăng khả năng phát hiện và điều tra sự cố thông qua các phương thức phân tích nâng cao như đẩy file trực tiếp lên các sandbox như totalvirus hoặc hệ thống tương tự/check IP reputation/kéo thả các thông tin sang các hệ thống Vul Scanning khác để đưa ra các tương quan hoặc Kill chain attack/…
13	Khả năng phân tích, điều tra sự cố.	Cung cấp các báo cáo phân tích về hành vi người dùng (User Behavior Analysis) và hoạt động của hệ thống một cách tổng quan nhằm hỗ trợ việc kiểm toán, chống lại các hành vi can thiệp dữ liệu.

		Cung cấp công cụ điều tra để phát hiện các hành vi bất thường trên các hệ thống bị xâm nhập (phục vụ cho việc điều tra số).
14	Khả năng quản lý sự cố	Có khả năng ghi nhớ các câu lệnh tìm kiếm, các bước đã thực hiện, các gợi ý cho việc xử lý, ứng phó sự cố.
		Có khả năng xâu chuỗi các sự kiện liên quan đến sự cố theo thời gian để hiểu rõ về vòng đời của cuộc tấn công.
		Có khả năng giám sát và xâu chuỗi các sự kiện từ "điểm đầu" tới "điểm cuối" của một sự cố thành một "workflow".
		Cho phép tích hợp các hệ thống SOAR (Security Orchestration Automation and Response) thực hiện quá trình tự động phản ứng lại các dấu hiệu bất thường như thu thập thông tin chuyên sâu, cho phép kết nối tới các hãng thứ ba để thực hiện ngăn chặn.
		Cho phép triển khai tích hợp cơ chế cảnh báo qua đa nền tảng như MS Team, Email…
15	Khả năng quản lý rủi ro	Ngoài các cảnh báo (alerts) được thiết lập, hệ thống giám sát cung cấp bổ sung dashboard theo dõi các sự kiện bất thường thông qua các chỉ số bảo mật (security indicator) từ đó hiểu và chủ động quản lý rủi ro tổng thể.
		Cam kết triển khai đối với tài khoản đặc quyền trong hệ thống, các hoạt động của tài khoản đặc quyền ngoài giờ làm việc cần có cơ chế tự động phát hiện các truy vấn bất thường.
16	Các yêu cầu khác	Có các dashboard/report cho phép tra cứu lịch sử hoạt động của tài khoản người dùng trong vòng tối thiểu 90 ngày bao gồm các hoạt động truy cập của tài khoản, các địa chỉ truy cập từ đâu, các máy chủ trong hệ thống đã truy cập và các kết nối truy cập.
III	**Yêu cầu bản quyền các tính năng khác**	
1	Khả năng quản lý lỗ hổng tổng thể	Cho phép tích hợp với hệ thống quản lý lỗ hổng hoặc thông tin tình báo mạng để theo dõi trạng thái và hoạt động của các lỗ hổng tồn tại trên hệ thống.
2	Mô hình hóa kiến trúc mạng	Cho phép mô hình hóa lại kiến trúc mạng, qua đó biết được tình trạng an ninh tại từng thành phần trong hạ tầng mạng theo thời gian thực.

Ghi chú: Các model, xuất xứ (nếu có) trong E-HSMT này chỉ mang tính chất tham khảo, nhà thầu có thể chào hàng hóa/dịch vụ tương đương hoặc tốt hơn so với yêu cầu của E-HSMT.

b) Yêu cầu về nhân sự thực hiện dịch vụ:

STT	Vị trí công việc	Số lượng	Kinh nghiệm trong các công việc tương tự	Chứng chỉ/trình độ chuyên môn[(2)]
1	Quản lý dự án	1	Tối thiểu 05 năm kinh nghiệm hoặc tối thiểu 02 hợp đồng	i) Bằng cấp: Đại học chuyên ngành Công nghệ thông tin/ An toàn thông tin hoặc chuyên ngành gần với Công nghệ thông tin theo quy định tại Khoản 1,2 Điều 2 Thông tư số 08/2022/TT-BTTTT ngày 30/6/2022 ii) Chứng chỉ: + Có tối thiểu 01 trong các chứng chỉ quản lý dự án sau: PMP, PSM, PMI-RMP hoặc tương đương. *(Các chứng chỉ phải còn hiệu lực đến thời điểm đóng thầu.)* iii) Kinh nghiệm trong các công việc tương tự: Có tối thiểu 05 năm kinh nghiệm trong lĩnh vực An toàn thông tin tính từ thời điểm tốt nghiệp đại học hoặc đã tham gia tối thiểu 02 hợp đồng trong lĩnh vực An toàn thông tin với vị trí quản lí dự án *(Nhà thầu kèm theo văn bản xác nhận của Chủ đầu tư/đại diện Chủ đầu tư hoặc Quyết định phân công nhiệm vụ của nhà thầu (kèm theo Hợp đồng) hoặc các tài liệu có tính pháp lý tương đương).*
2	SOC Manager/ Trưởng nhóm giám sát ATTT	1	Tối thiểu 05 năm hoặc tối thiểu 03 hợp đồng	i) Bằng cấp: Đại học chuyên ngành Công nghệ thông tin/ An toàn thông tin hoặc chuyên ngành gần với Công nghệ thông tin theo quy định tại Khoản 1,2 Điều 2 Thông tư số 08/2022/TT-BTTTT ngày 30/6/2022 ii) Chứng chỉ: có tối thiểu 01 trong các chứng chỉ về an toàn thông tin sau: CISM, CHFI, GREM, CISSP, GISPO hoặc tương đương. *(Các chứng chỉ phải còn hiệu lực đến thời điểm đóng thầu.)*

				iii) Kinh nghiệm trong các công việc tương tự: Có tối thiểu 05 năm kinh nghiệm trong lĩnh vực An toàn thông tin tính từ thời điểm tốt nghiệp đại học hoặc đã tham gia tối thiểu 03 hợp đồng giám sát An ninh thông tin với vị trí SOC Manager *(Nhà thầu kèm theo văn bản xác nhận của Chủ đầu tư/đại diện Chủ đầu tư hoặc Quyết định phân công nhiệm vụ của nhà thầu (kèm theo Hợp đồng) hoặc các tài liệu có tính pháp lý tương đương).*
3	Nhân sự triển khai giải pháp	3	Tối thiểu 03 năm hoặc tối thiểu 01 hợp đồng	i) Bằng cấp: Đại học chuyên ngành Công nghệ thông tin/ An toàn thông tin hoặc chuyên ngành gần với Công nghệ thông tin theo quy định tại Khoản 1,2 Điều 2 Thông tư số 08/2022/TT-BTTTT ngày 30/6/2022. ii) Chứng chỉ: + 02 nhân sự mỗi nhân sự phải có tối thiểu 01 chứng chỉ chuyên môn của giải pháp được đề xuất hoặc tương đương trong lĩnh vực triển khai/ quản trị/ vận hành hệ thống SIEM. + Ưu tiên có 01 trong các chứng chỉ chuyên môn của giải pháp được đề xuất như: Architect, Enterprise Security, Security Expert hoặc tương đương. *(Các chứng chỉ phải còn hiệu lực đến thời điểm đóng thầu.)* iii) Kinh nghiệm trong các công việc tương tự: Có tối thiểu 03 năm kinh nghiệm trong lĩnh vực An toàn thông tin tính từ thời điểm tốt nghiệp đại học hoặc đã tham gia tối thiểu 01 hợp đồng An ninh thông tin với vị trí nhân sự triển khai giải pháp *(Nhà thầu kèm theo văn bản xác nhận của Chủ đầu tư/đại diện Chủ đầu tư hoặc Quyết định phân công nhiệm vụ của nhà thầu (kèm theo Hợp đồng) hoặc các tài liệu có tính pháp lý tương đương).*
4	Nhân sự giám sát ATTT (Tier 1)	6	Tối thiểu 01 năm hoặc tối thiểu 01 hợp đồng	i) Bằng cấp: Đại học chuyên ngành Công nghệ thông tin/ An toàn thông tin hoặc chuyên ngành gần với Công nghệ thông tin theo quy định tại Khoản 1,2 Điều 2 Thông tư số 08/2022/TT-BTTTT ngày 30/6/2022 ii) Chứng chỉ: Mỗi nhân sự phải có tối thiểu 01 trong các chứng chỉ ATTT sau: CEH, EHE, ICIP,

				CCNA, ComTIA CySA+, CompTIA Security+, CyberOps Associate hoặc tương đương *(Các chứng chỉ phải còn hiệu lực đến thời điểm đóng thầu.)* iii) Kinh nghiệm trong các công việc tương tự: Có tối thiểu 01 năm kinh nghiệm trong lĩnh vực An toàn thông tin tính từ thời điểm tốt nghiệp đại học hoặc đã tham gia tối thiểu 01 hợp đồng giám sát An ninh thông tin *(Nhà thầu kèm theo văn bản xác nhận của Chủ đầu tư/đại diện Chủ đầu tư hoặc Quyết định phân công nhiệm vụ của nhà thầu (kèm theo Hợp đồng) hoặc các tài liệu có tính pháp lý tương đương).*
5	Nhân sự phân tích an toàn thông tin (Tier 2)	2	Tối thiểu 03 năm hoặc tối thiểu 01 hợp đồng	i) Bằng cấp: Đại học chuyên ngành Công nghệ thông tin/ An toàn thông tin hoặc chuyên ngành gần với Công nghệ thông tin theo quy định tại Khoản 1,2 Điều 2 Thông tư số 08/2022/TT-BTTTT ngày 30/6/2022 ii) Chứng chỉ: Mỗi nhân sự có tối thiểu 01 trong các chứng chỉ ATTT sau: CHFI, CTIA, OSCP, OSWE, GCIH hoặc tương đương. *(Các chứng chỉ phải còn hiệu lực đến thời điểm đóng thầu.)* iii) Kinh nghiệm trong các công việc tương tự: Có tối thiểu 03 năm kinh nghiệm trong lĩnh vực An toàn thông tin tính từ thời điểm tốt nghiệp đại học hoặc đã tham gia tối thiểu 01 hợp đồng An toàn thông tin*(Nhà thầu kèm theo văn bản xác nhận của Chủ đầu tư/đại diện Chủ đầu tư hoặc Quyết định phân công nhiệm vụ của nhà thầu (kèm theo Hợp đồng) hoặc các tài liệu có tính pháp lý tương đương).*
6	Nhân sự phân tích và xử lý sự cố (Tier 3)	3	Tối thiểu 05 năm hoặc tối thiểu 02 hợp đồng	i) Bằng cấp: Đại học chuyên ngành Công nghệ thông tin/ An toàn thông tin hoặc chuyên ngành gần với Công nghệ thông tin theo quy định tại Khoản 1,2 Điều 2 Thông tư số 08/2022/TT-BTTTT ngày 30/6/2022 ii) Chứng chỉ: Mỗi nhân sự có tối thiểu 01 chứng chỉ về an toàn thông tin sau: OSCP, OSEP, OSWE, CHFI, GCFE, GCFA hoặc tương đường.

				Các chứng chỉ còn hiệu lực đến thời điểm đóng thầu. *(Các chứng chỉ phải còn hiệu lực đến thời điểm đóng thầu.)* iii) Kinh nghiệm trong các công việc tương tự: Có tối thiểu 05 năm kinh nghiệm trong lĩnh vực An toàn thông tin tính từ thời điểm tốt nghiệp đại học hoặc đã tham gia tối thiểu 02 hợp đồng An toàn thông tin *(Nhà thầu kèm theo văn bản xác nhận của Chủ đầu tư/đại diện Chủ đầu tư hoặc Quyết định phân công nhiệm vụ của nhà thầu (kèm theo Hợp đồng) hoặc các tài liệu có tính pháp lý tương đương).*

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;

2. Kế hoạch công tác.

3. Ngoài ra, nhà thầu phải đính kèm theo E-HSDT Bảng tuyên bố đáp ứng theo mẫu dưới đây

Mẫu Bảng tuyên bố đáp ứng kỹ thuật

STT	**Yêu cầu tại theo E-HSMT**	**Hồ sơ tham chiếu**	**Tính đáp ứng dịch vụ của nhà thầu**
(1)	(2)	(3)	(4)
I	**Yêu cầu chung của dịch vụ**	"Tên tài liệu" - "Phần, chương, mục, bảng (nếu có)" - "trang"	Đáp ứng
1	**Yêu cầu hiệu năng**	….	….
	….	…..	…

Ghi chú:

- Nội dung ở các cột (1), (2), phải được lập tương ứng với nội dung của yêu cầu kỹ thuật của gói thầu tại mục 3 Chương này.

- Cách thức trình bày nội dung ở cột (3) như sau: "Tên tài liệu" - "Phần, chương, mục, bảng (nếu có)" - "trang"

- Nội dung ở cột (4) chỉ được ghi "Đáp ứng" hoặc "Không đáp ứng".

5. Yêu cầu về Báo cáo

+ Báo cáo định kỳ theo tuần, tháng, quý về tình hình giám sát và xử lý sự cố.

+ Báo cáo phân tích và xử lý sự cố đối với các sự cố ở mức nghiêm trọng (Trong phạm vi gói thầu này, các sự cố ở mức nghiêm trọng được hiểu là những sự cố an toàn thông tin có mức độ từ 'nghiêm trọng' trở lên, được xác định và phân loại theo quy định hiện hành của VCBS)

+ Báo cáo phân tích về hành vi người dùng (User Behavior Analysis).

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

+ Trong vòng 07 ngày làm việc kể từ khi Nhà thầu hoàn thành toàn bộ công việc của hợp đồng bao gồm: triển khai cài đặt, tích hợp và thu thập log từ các thiết bị/ hệ thống trong phạm vi yêu cầu, đảm bảo chức năng giám sát an toàn thông tin hoạt động đầy đủ, Chủ đầu tư và Nhà thầu sẽ ký biên bản nghiệm thu tổng thể dự án.

7. Quy định về bảo mật thông tin.

- Nhà thầu cam kết không tiết lộ bất kỳ thông tin, dữ liệu hoặc tài liệu nào có chứa các thông tin, dữ liệu như sau:

+ Thông tin, dữ liệu của VCBS và của các hệ thống trong phạm vi triển khai cung cấp dịch vụ;

+ Thông tin, dữ liệu hình thành trong quá trình triển khai cung cấp dịch vụ.

+ Chịu trách nhiệm nếu để xảy ra việc lộ lọt thông tin dữ liệu của Chủ đầu tư trong quá trình triển khai cung cấp dịch vụ do lỗi của đơn vị và của các nhân sự tham gia vào dự án.

+ Chỉ sử dụng các các nhân sự tham gia vào dự án theo đề xuất của đơn vị, cam kết không sử dụng các nhân sự khác khi chưa được sự đồng ý của Chủ đầu tư.

8. Yêu cầu về chất lượng dịch vụ :

Nhà thầu có cam kết đảm bảo các yêu cầu về chất lượng dịch vụ như sau:

Thời gian xử lý cảnh bảo, kiểm tra xác minh phân loại cảnh báo, tạo ticket gán yêu cầu xử lý cho bộ phân tương ứng:

- Xử lý cảnh báo mất ATTT CẤP ĐỘ NGHIÊM TRỌNG tối đa không quá 30 phút.
- Xử lý cảnh báo mất ATTT CẤP ĐỘ CAO tối đa không quá 1 giờ.
- Xử lý cảnh báo mất ATTT CẤP ĐỘ TRUNG BÌNH tối đa không quá 2 giờ.
- Xử lý cảnh báo mất ATTT CẤP ĐỘ THẤP tối đa không quá 24 giờ