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:

1.1. Giới thiệu về dự toán mua sắm

- Tên dự toán mua sắm: Triển khai nâng cấp, mở rộng "Hệ thống đảm bảo an toàn thông tin theo mô hình "4 Lớp" của Sở Tài chính";

- **Quyết định phê duyệt Kế hoạch lựa chọn nhà thầu:** Quyết định số 14029/QĐ-STC ngày 06/11/2025 của Sở Tài chính Hà Nội về việc phê duyệt kế hoạch lựa chọn nhà thầu triển khai nâng cấp, mở rộng "Hệ thống đảm bảo an toàn thông tin theo mô hình "4 Lớp" của Sở Tài chính".

1.2. Giới thiệu về gói thầu

- Chủ đầu tư: Sở Tài chính thành phố Hà Nội

- Tên gói thầu: Triển khai nâng cấp, mở rộng "Hệ thống đảm bảo an toàn thông tin theo mô hình "4 Lớp" của Sở Tài chính".

- Hình thức lựa chọn nhà thầu: Đấu thầu rộng rãi trong nước, qua mạng.

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

- Nguồn vốn: Ngân sách Nhà nước

- Thời gian thực hiện hợp đồng: Quý IV/2025

- Loại hợp đồng: Trọn gói

- Nội dung công việc gói thầu: Triển khai nâng cấp, mở rộng "Hệ thống đảm bảo an toàn thông tin theo mô hình "4 Lớp" của Sở Tài chính"

2. Mục tiêu công việc:

- Nâng cao nhận thức ATTT của người dùng cuối, giúp học viên nắm được các kiến thức cơ bản về An toàn thông tin để tự bảo đảm ATTT trong công việc thường ngày và cuộc sống số.

- Có nhận thức đúng đắn và sử dụng hợp lý các nguồn tài nguyên CNTT tránh gặp phải các sự cố gây mất ATTT.

- Nhận biết các hiểm họa và rủi ro ATTT thường trực đe dọa hoạt động và tài sản của tổ chức trong hoạt động thường ngày, sử dụng ngân sách hợp lý hơn cho việc đảm bảo An ninh thông tin và hoạt động thông suốt của tổ chức.

- Phối hợp tốt hơn với các bộ phận liên quan khi đề xuất, phê duyệt, triển khai các dự án về ATTT.

+ Cung cấp các tri thức, thông tin:

- Các kiến thức nền tảng về an toàn thông tin

- Sử dụng internet an toàn

- Phòng chống tấn công mạng.

3. Yêu cầu kỹ thuật của gói thầu:

Chi tiết khối lượng công việc và yêu cầu kỹ thuật của gói thầu*:* Bất kỳ thương hiệu, mã hiệu (nếu có) trong bảng yêu cầu kỹ thuật dưới đây để minh họa các tiêu chuẩn chất lượng, tính năng kỹ thuật yêu cầu, nhà thầu có thể lựa chọn dự thầu hàng hóa có nguồn gốc, xuất xứ, nhà sản xuất, thương hiệu, mã hiệu phù hợp với điều kiện cung cấp nhưng phải đảm bảo yêu cầu có tiêu chuẩn kỹ thuật, đặc tính kỹ thuật, tính năng sử dụng "tương đương" hoặc "ưu việt hơn" so với các yêu cầu tối thiểu.

STT	Danh mục	Mô tả	Phạm vi	ĐVT	Số lượng	Ghi chú
1	**Dịch vụ diễn tập ATTT**	Tổ chức diễn tập mô phỏng lại các tình huống, kịch bản tấn công trong thực tế nhằm trang bị các kĩ năng ứng cứu sự cố và nâng cao hiệu quả phối hợp xử lý giữa các thành viên trong đội ngũ an toàn thông tin tại Sở. Diễn tập theo hình thức tấn công phòng thủ.	Tổ chức diễn tập cho cán bộ của đơn vị. - Phạm vi: 1 ứng dụng/website - Thực hiện theo hình thức: Tấn công phòng thủ. - Thời gian diễn tập: 01 ngày	Gói	1	- Khảo sát hiện trạng an toàn thông tin: Khảo sát hệ thống thực hiện diễn tập thực chiến và các hệ thống, thông tin liên quan. - Xây dựng môi trường diễn tập cho việc diễn tập và phải phản ánh gần đúng nhất môi trường đang vận hành thực tế của Sở (ít nhất phải bao gồm các nghiệp vụ, hệ thống quan trọng của Sở và phải giả lập được các gói tin giao dịch thông thường của người dùng cuối ví dụ: gởi/ nhận thư điện tử, duyệt web, truy cập ứng dụng…). - Yêu cầu môi trường có đầy đủ máy work-stations, laptops, hệ thống mạng, các thiết bị mạng, firewall, thiết bị bảo mật, hệ thống email…đang được sử dụng tại Sở. - Xây dựng tài liệu phục vụ diễn tập (xây dựng một kịch bản chi tiết bao gồm các tình huống phụ bao gồm diễn tập, quy trình diễn tập, hướng dẫn diễn tập, đánh giá rủi ro và phương án xử lý rủi ro trong diễn tập). - Chuẩn bị kỹ lưỡng, bài bản, sẵn sàng các phương án bảo vệ nhằm giảm thiểu rủi ro, bảo đảm hệ thống luôn được an toàn trong quá trình diễn tập.

STT	Danh mục	Mô tả	Phạm vi	ĐVT	Số lượng	Ghi chú
						- Xác định rõ hệ thống là mục tiêu diễn tập, công cụ, kỹ thuật được sử dụng đảm bảo không gây hậu quả hoặc hậu quả xảy ra trong giới hạn cho phép. - Các cán bộ đối tượng tham gia trực tiếp thực hiện ứng phó khi có sự cố xảy ra trên môi trường giả lập mà nhà cung cấp xây dựng theo kịch bản, quy trình diễn tập đề xuất.
2	**Gói dịch vụ Giám sát ATTT MSS**	Nền tảng giám sát, quản lý an toàn thông tin hỗ trợ cho doanh nghiệp, tổ chức; kịp thời phát hiện, xử lý, ứng cứu các rủi ro gây mất an toàn thông tin, lộ lọt dữ liệu, trước các cuộc tấn công từ trong và ngoài tổ chức.	- Router: 2 - Switch: 2 - LB: 1 - FW L4: 1 - IDS/IPS: 2 - Server monitor (Windows + Sysmon + Web server): 9	EPS/ tháng	497	- Giám sát, cảnh báo 24/7 trước những sự cố an toàn thông tin; - Thực hiện các điều tra, truy vết nguồn tấn công triệt để; - Giúp đơn vị tối ưu hóa về thời gian, công sức và chi phí cũng như hiệu quả trong việc quản trị an toàn thông tin; - Xây dựng và hệ thống qua các chỉ số an toàn thông tin (security index) giúp tổ chức nắm bắt được hiện trạng và xu hướng an toàn thông tin. - Báo cáo chi tiết theo tuần/tháng/quý - Hỗ trợ xử lý sự cố an toàn thông tin - Dashboard tổng hợp tình hình giám sát an toàn thông tin

STT	Danh mục	Mô tả	Phạm vi	ĐVT	Số lượng	Ghi chú
2.1	**Thiết bị tường lửa**	Thiết bị phòng chống tấn công xâm nhập IPS (Hoặc tương đương)	(1) FG 120-BDL-950-12-Hardware plus FortiCare Premium and FortiGuard Unified Threat Protection (UTP) - 18 x GE RJ45 ports (including 1 x MGMT port, 1 X HA port, 16 x switch ports), 8 x GE SFP slots, 4 x 10GE SFP+ slots, SP5 hardware accelerated, dual AC power supplies; (2) FC-10-F120G-585-02-12 (1 năm)'- FortiAnalyzer Cloud: cloud-Based central logging & analytics. Include All FortiGate log types, IOC Service, Security Automation Service and FortiGuard Outbreak Detection Service; (3) FC1-10-AZCLD-1118-01-DD-'Generative AI powered security service utilizing large language models (LLMs) for real-time assistance in SOC analysis, incident investigation, triage and response for 5 GB/Day subscription;	Thiết bị	1	

STT	Danh mục	Mô tả	Phạm vi	ĐVT	Số lượng	Ghi chú
			(4) FC1-10-AITAZ-1089-02-DD-FortiAI Assistant upgrade license for adding 500,000 AI tokens Hoặc tương đương			

STT	Danh mục	Mô tả	Phạm vi	ĐVT	Số lượng	Ghi chú
2.2	**Thiết bị Sensor**	Thiết bị để thu thập log lớp mạng (network)	Single AMD EPYC™ 4004 / Ryzen™ 7000 Series Processors Dual Channel DDR5 ECC/Non-ECC UDIMM, 4 x DIMMs 2 x 1Gb/s LAN ports via Broadcom® BCM5720 4 x 3.5"/2.5" SATA hot-swappable bays 1 x M.2 slot with PCIe Gen4 x4 interface 1 x FHFL PCIe Gen5 x16 slot 1 x FHHL PCIe Gen4 x4 slot 1+1 550W 80 PLUS Platinum redundant power supplies 1 x AMD Ryzen™ 9 7900 (12C/24T , 3.8GHz) 2 x RAM Kingston Fury DDR5 8GB 5200MHz UDIMM ECC 2 x Samsung PM893 960GB SATA3 for Enterprise 1 x LSI 9361-8i, RAID Level 0,1,5,6 Hoặc tương đương	Thiết bị	1	

STT	Danh mục	Mô tả	Phạm vi	ĐVT	Số lượng	Ghi chú
2.3	**Thiết bị EC (Event collector)**	Thiết bị để thu thập log từ các thiết bị, máy chủ,…	Dual 2nd/1st Gen Intel® Xeon® Scalable Processors 6-Channel DDR4 RDIMM/LRDIMM, 16 x DIMMs 2 x 1Gb/s LAN ports via Intel® I210-AT 4 x 3.5"/2.5" SATA/SAS hot-swappable bays 1 x 2.5" SATA Internal fixed bay 2 x 2.5" SATA Internal fixed bays (optional) 2 x SATA DOMs supported 2 x M.2 slots with PCIe Gen3 x4 interface 2 x FHHL PCIe Gen3 x16 slots Single 550W 80 PLUS Platinum hot-swap power supply 1 x Intel® Xeon® Silver 4216 (16C/32T , 2.1GHz) 1 x Samsung DDR4 2Rx4 16GB 2666 ECC RDIMM 2 x Samsung PM893 960GB SATA3 for Enterprise 1 x LSI 9361-8i, RAID Level 0,1,5,6 Hoặc tương đương	Thiết bị	1	
3	**Dịch vụ kiểm thử xâm nhập**	Hình thức đánh giá: một trong 03 hình thức:	Các ứng dụng, website của sở Tài chính: Cổng thông tin điện tử; Cơ sở dữ liệu về giá; Cơ sở dữ liệu tài	Trang web	5	**- Thực hiện 1 lần trong 1 năm** **- Mục tiêu**: + Tấn công, kiểm thử phát hiện các điểm yếu

STT	Danh mục	Mô tả	Phạm vi	ĐVT	Số lượng	Ghi chú
	đánh giá ATTT	GrayBox, BlackBox, WhiteBox.	sản công lĩnh vực hành chính sự nghiệp thành phố Hà Nội; Cơ sở dữ liệu văn bản quản lý nhà nước ngành tài chính; Hệ thống cơ quan điện tử.			bảo mật tồn tại bên trong hệ thống thông tin và ứng dụng thông qua các dịch vụ được tùy biến theo từng điều kiện khách hàng bao gồm : Đánh giá điểm yếu, kiểm thử xâm nhập. + Rà soát các lỗ hổng, điểm yếu trong các hệ thống phần mềm, ứng dụng web, … của Chủ đầu tư, nhằm giảm thiểu tối đa các lỗ hổng tồn tại trong hệ thống trước khi bị kẻ xấu lợi dụng. + Tư vấn cho khách hàng các phương pháp lập trình phần mềm an toàn, cách bảo vệ mã nguồn phần mềm trước việc dịch ngược mã nguồn. **- Thực hiện một trong các phương pháp:** + Kiểm thử hộp đen - Black box: Không được cung cấp bất cứ thông tin nào về mục tiêu kiểm thử, đóng vai trò như một hacker bên ngoài -> Rò quét, tìm kiếm một phần lỗ hổng hệ thống + Kiểm thử hộp xám - Gray box: Được cung cấp một phần thông tin về mục tiêu kiểm thử (tài khoản người dùng, thông tin hệ thống), đóng vai trò như người dùng thông thường -> Rò quét, tìm kiếm một phần lỗ hổng hệ thống Đánh giá các lỗ hổng leo thang, vượt quyền trên ứng dụng, hệ thống. + Kiểm thử hộp trắng - White box: Được cung cấp đầy đủ thông tin (mã nguồn, tài khoản quản trị, thông tin chi tiết hệ thống), đóng vai trò như quản trị hệ thống -> Rò quét, tìm kiếm tối đa lỗ
		Kiểm tra bảo mật ứng dụng Wep App				
		+ Kiểm thử xâm nhập theo OWASP Top 10 cho Web				
		- A1: Injection				
		- A2: Broken Authentication				
		- A3: Sensitive Data Exposure				
		- A4: XML External Entities (XXE)				
		- A5: Broken Access Control				

STT	Danh mục	Mô tả	Phạm vi	ĐVT	Số lượng	Ghi chú
		- A6: Security Misconfiguration				hổng hệ thống -> Đánh giá toàn diện về các lỗ hổng bên trong và bên ngoài **- Phương thức triển khai:** 1. Chủ đầu tư cung cấp thông tin liên quan đến hệ thống/website/ ứng dụng cần đánh giá an toàn thông tin. 2. Đơn vị cung cấp dịch vụ thực hiện đánh giá an toàn thông tin lần 1. 3. Chủ đầu tư thực hiện vá, khắc phục lỗ hổng, điểm yếu bảo mật do đơn vị cung cấp dịch vụ tìm ra. 4. Đơn vị cung cấp dịch vụ thực hiện đánh giá lại. 5. Đơn vị cung cấp dịch vụ gửi kết quả tái đánh giá (và cấp chứng nhận cho Chủ đầu tư nếu hệ thống đó được đánh giá bằng phương pháp whitebox). **- Các bước kiểm thử xâm nhập theo OWASP cho ứng dụng web:** + Thu thập thông tin ứng dụng + Kiểm tra cấu hình (SSL/TLS, CSDL, cấu hình máy chủ web, ...) + Kiểm tra phần xác thực + Kiểm tra quản lý phiên giao dịch + Kiểm tra cấp quyền + Kiểm tra phê chuẩn dữ liệu đầu vào + Kiểm tra việc sử dụng mật mã + Kiểm tra các lỗi business logic
		- A7: Cross Site Scripting (XSS)				
		- A8: Insecure Deserialization				
		- A9: Using Components with Known Vulnerabilities				
		- A10: Insufficient Logging & Monitoring				
		+ Kiểm thử xâm nhập các lỗ hổng khác, sử dụng các kỹ thuật thủ công và tự động				

STT	Danh mục	Mô tả	Phạm vi	ĐVT	Số lượng	Ghi chú
4	**Sản phẩm ATTT Smart IR**	Giải pháp phát hiện và ứng cứu sự cố điểm cuối toàn diện cho phép bảo vệ máy chủ, máy trạm chống các loại virus, mã độc; hỗ trợ truy vấn, điều tra nguyên nhân và ứng cứu kịp thời khi có sự cố về an toàn thông tin; giám sát việc cài đặt phần mềm trái phép và giám sát việc tuân thủ các chính sách bảo mật của các tổ chức, doanh nghiệp.	Số lượng: 242 máy trạm	License/ năm	242	**Các tính năng chính:** - Phát hiện, cách ly, xóa bỏ các loại mã độc: virus, mã độc mã hóa tống tiền (ransomeware), lừa đảo (phishing), thư rác…. - Giám sát các sự kiện, tiến trình, phân tích hành vi trên máy tính, phát hiện bất thường. - Kiểm soát tuân thủ các quy định an toàn thông tin tại máy tính người dùng. - Giám sát việc cài đặt, sử dụng phần mềm được phép/không được phép. - Cho phép chia sẻ thông tin, dữ liệu thống kê tình hình lây nhiễm mã độc với hệ thống kỹ thuật của cơ quan chức năng có thẩm quyền. - Phát hiện và phản hồi các mối nguy hại tại điểm cuối (Endpoint Detection & Response – EDR). - Quản lý tập trung, quản trị người dùng và thiết bị đầu cuối. - Hỗ trợ cài đặt trên các hệ điều hành: Windows, Linux

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.

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

Mục này quy định về quy trình kiểm tra, nghiệm thu sản phẩm, trình tự giao nộp sản phẩm (nếu có)... để phục vụ công tác thanh, quyết toán hợp đồng.