Chương V. YÊU CẦU VỀ KỸ THUẬT

1. Giới thiệu chung về gói thầu:

Tên Chủ đầu tư: Trung tâm Phát triển Khoa học, Công nghệ và Đổi mới sáng tạo tỉnh Thái Nguyên

Tên gói thầu: Dịch vụ giám sát an toàn thông tin chuyên nghiệp cho các hệ thống thông tin tại Trung tâm Dữ liệu tỉnh

Tên dự án/dự toán mua sắm: Dịch vụ giám sát an toàn thông tin chuyên nghiệp cho các hệ thống thông tin tại Trung tâm Dữ liệu tỉnh

2. Mục tiêu công việc:

Thuê đơn vị cung cấp dịch vụ giám sát an toàn thông tin cho các hệ thống thông tin tại Trung tâm Dữ liệu tỉnh nhằm đảm bảo việc vận hành hệ thống thông tin, chống các cuộc tấn công phát sinh từ trong và ngoài mạng.

3. Yêu cầu kỹ thuật của gói thầu:

3.1. Nhà thầu cung cấp dịch vụ cần đáp ứng được các yêu cầu tối thiểu sau:

STT	Danh mục	Tính năng	Đơn vị tính	Số lượng
1	Dịch vụ giám sát an toàn thông tin cho các hệ thống thông tin tại Trung tâm Dữ liệu tỉnh Thái Nguyên	**1. Giám sát An toàn thông tin cho hạ tầng công nghệ thông tin, các hệ thống thông tin của tỉnh đặt tại Trung tâm dữ liệu tỉnh Thái Nguyên:** - Số lượng máy chủ giám sát tối đa: 200 máy chủ. - Thu thập log từ các thiết bị mạng. - Chủ động theo dõi, phát hiện sớm các nguy cơco mất an toàn thông tin mạng để kịp thời xử lý, khắc phục. - Phân tích, phân loại sự kiện, sự cố an toàn thông tin mạng chuyên sâu. - Nghiên cứu, cập nhật, điều chỉnh hệ thống giám sát phù hợp điều kiện thực tế và kỹ thuật tấn công mới. - Thiết lập hệ thống cảm biến giám sát. - Triển khai kênh kết nối giám sát. Vận hành và trực hệ thống giám sát an toàn thông tin mạng 24/7. Thiết lập hệ thống theo dõi, giám sát cho cán bộ trực vận hành Trung tâm Dữ liệu và hướng dẫn cán bộ của Trung tâm dùng các công cụ giám sát, phát hiện sự cố. Thiết lập hệ thống cảnh báo về Mail và SMS.	Tháng	9

STT	Danh mục	Tính năng	Đơn vị tính	Số lượng
		- Tổng hợp đánh giá kết quả giám sát theo ngày. Kết nối dữ liệu về Trung tâm Giám sát an toàn không gian mạng quốc gia (khi có yêu cầu). - Hỗ trợ diễn tập An toàn thông tin tối thiểu 1 lần/năm **2. Trường hợp phát hiện các hành vi rà quét, tấn công mạng, điểm yếu, lỗ hổng bảo mật:** - Ngay lập tức thông báo với chủ đầu tư và cử nhóm kỹ thuật tiến hành xử lý. - Đề xuất phương án xử lý, chủ động cách ly các máy chủ nghi ngờ nhiễm mã độc. - Phân tích, tìm ra nguyên nhân, khắc phục các lỗ hổng trong thời gian sớm nhất khi xảy ra sự cố tấn công mạng. - Hỗ trợ tư vấn, hướng dẫn cách thức xử lý rà quét trên các máy chủ nghi ngờ hoặc các máy chủ được chủ đầu tư yêu cầu - Cung cấp đường dây nóng hỗ trợ 24/24 giờ. - Cách ly chủ động các máy chủ khi có yêu cầu. - Rà quét đột xuất các máy chủ khi có yêu cầu. - Hỗ trợ xây dựng quy trình xử lý đối với các sự cố mất an toàn thông tin tại Trung tâm Dữ liệu tỉnh. - Hỗ trợ đánh giá lỗ hổng bảo mật cho một số hệ thống thông tin, WebSite khi có yêu cầu. **3. Thực hiện tổng hợp, xây dựng báo cáo tuần, tháng và báo cáo đột xuất theo yêu cầu**		

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:

Việc nghiệm thu, đánh giá chất lượng của sản phẩm dựa trên yêu cầu của E-HSMT, cam kết của nhà thầu trong E-HSDT, và các quy định của pháp luật.