TỈNH ỦY ĐỒNG NAI
VĂN PHÒNG
*
Số [so] -TTr/VPTU

ĐẢNG CỘNG SẢN VIỆT NAM

Đồng Nai, ngày [ng]tháng 4 năm 2023

TỜ TRÌNH

Về việc xin chủ trương thuê Dịch vụ công nghệ thông tin Giải pháp đảm bảo an toàn thông tin cho hệ thống Công nghệ thông tin tại Trung tâm tích hợp dữ liệu của Tỉnh ủy

Kính gửi: Ủy ban nhân dân tỉnh Đồng Nai.

Căn cứ Nghị định số 73/2019/NĐ-CP ngày 05/9/2019 của Chính phủ quy định quản lý đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước;

Căn cứ Nghị định số 142/2016/NĐ-CP ngày 14/10/2016 của Chính phủ về Ngăn chặn xung đột thông tin trên mạng;

Căn cứ 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;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Căn cứ Thông tư số 03/2020/TT-BTTTT ngày 24/02/2020 của Bộ Thông tin Truyền thông về Quy định về lập đề cương và dự toán chi tiết đối với hoạt động ứng dụng công nghệ thông tin sử dụng kinh phí chi thường xuyên thuộc nguồn vốn ngân sách nhà nước;

Căn cứ Thông tư số 04/2020/TT-BTTTT ngày 24/02/2020 của Bộ Thông tin và Truyền thông quy định về lập và quản lý chi phí dự án đầu tư ứng dụng công nghệ thông tin;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông 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 theo cấp độ và hướng dẫn chi tiết tại 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;

Căn cứ Quyết định số 1017/QĐ-TTg ngày 14/8/2018 của Thủ tướng Chính phủ về việc Phê duyệt Đề án giám sát an toàn thông tin mạng đối với hệ thống,

dịch vụ công nghệ thông tin phục vụ Chính phủ điện tử đến năm 2020, định hướng đến năm 2025;

Căn cứ Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông Quy định hoạt động giám sát an toàn thống thông tin;

Căn cứ Chỉ thị số 14/CT-TTg ngày 07/6/2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam;

Căn cứ Chỉ thị số 60/CT-BTTTT ngày 16/09/2021 của Bộ Thông tin và Truyền thông ban hành về tổ chức triển khai diễn tập thực chiến bảo đảm an toàn thông tin mạng;

Căn cứ Quyết định số 1014/QĐ-BTTTT ngày 02/6/2022 của Bộ trưởng Bộ Thông tin và Truyền thông ban hành phê duyệt Đề án Bảo đảm an toàn thông tin cho đô thị thông minh giai đoạn 2022 - 2025;

Căn cứ Công văn số 2973/BTTTT-CATTT ngày 04/09/2019 của Bộ Thông tin và Truyền thông về việc "Hướng dẫn triển khai hoạt động giám sát an toàn thông tin trong cơ quan, tổ chức nhà nước";

Căn cứ Công văn số 235/CATTT-ATHTTT ngày 08/4/2020 của Cục An toàn thông tin, Bộ Thông tin và Truyền thông về Hướng dẫn Mô hình đảm bảo an toàn thông tin cấp Bộ, Tỉnh (mô hình 4 lớp);

Căn cứ Công văn số 1552/BTTTT-CATTT ngày 28/4/2020 của Bộ Thông tin và Truyền thông về việc Đôn đốc tổ chức triển khai bảo đảm an toàn thông tin cho hệ thống thông tin theo mô hình "4 lớp";

Căn cứ Quyết định số 27-QĐ/TW, ngày 10/8/2021 của Ban Bí thư ban hành kèm theo Chương trình ứng dụng công nghệ thông tin trong hoạt động của các cơ quan Đảng giai đoạn 2021 - 2025;

Căn cứ Nghị quyết số 05-NQ/TU ngày 28/3/2022 của Nghị quyết số 05-NQ/TU ngày 28/3/2022 của Ban Chấp hành Đảng bộ tỉnh về Chuyển đổi số tỉnh Đồng Nai đến năm 2025 và định hướng đến năm 2030;

Căn cứ Kế hoạch số 29/KH-UBND ngày 11/02/2022 của UBND tỉnh về Phát triển chính quyền số và bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Đồng Nai năm 2022,

Căn cứ Kế hoạch số 125-KH/TU ngày 17/3/2022 của Ban Thường vụ Tỉnh ủy về ứng dụng công nghệ thông tin trong hoạt động của các cơ quan đảng tỉnh Đồng Nai giai đoạn 2021 - 2025;

Căn cứ Kết luận của Ban Thường vụ Tỉnh ủy tại Công văn số 4704-CV/TU ngày 16/02/2023 về việc điều chỉnh các hạng mục và nguồn vốn trong Kế hoạch số 125-KH/TU ngày 17/3/2022 của Ban Thường vụ Tỉnh ủy;

Văn phòng Tỉnh Ủy kính trình Ủy ban nhân dân tỉnh xem xét, chấp thuận chủ trương thực hiện thuê Dịch vụ công nghệ thông tin Giải pháp đảm bảo an toàn thông tin cho hệ thống Công nghệ thông tin tại Trung tâm tích hợp dữ liệu của Tỉnh ủy, cụ thể như sau:

I. HIỆN TRẠNG VÀ SỰ CẦN THIẾT

1. Hiện trạng

Trong những năm qua, được sự quan tâm chỉ đạo của Tỉnh ủy, các cấp ủy đảng, hoạt động ứng dụng CNTT trong các cơ quan Đảng của tỉnh Đồng Nai đã mang lại những hiệu quả rõ rệt, đáp ứng kịp thời sự chỉ đạo, lãnh đạo điều hành của các cấp ủy đảng góp phần hoàn thành các nhiệm vụ chính trị quan trọng của tỉnh.

Năm 2019, Văn phòng Tỉnh ủy triển khai thực hiện hoạt động ứng dụng công nghệ thông tin, các thiết bị được trang bị sử dụng đúng mục đích, phù hợp với yêu cầu, tận dụng hạ tầng kỹ thuật sẵn có, trang bị đồng bộ hệ thống máy chủ và máy trạm và các trang thiết bị tin học, đảm bảo đưa vào khai thác sử dụng hợp lý, hiệu quả các trang thiết bị, tránh lãng phí trong đầu tư công.

Đặc biệt, trong năm 2021, Trung tâm tích hợp dữ liệu của các cơ quan Đảng được đầu tư, xây dựng đưa vào khai thác sử dụng gồm 03 máy chủ ảo hóa HPE DL380 Gen10, 02 thiết bị chuyển mạch SAN Switch - HPE 8/8 Base 8-port Enabled SAN Switch, 02 thiết bị lưu trữ San Storage MSA 2052 SAN DC ME SFF, 02 thiết bị chuyển mạch trung tâm CoreSwith-FF 5700 - 32 port 1/10Gb Base - T + 8 port 10 Gb SFP+ 2-port 40Gb-Stackable - Layer 3 - DCB-FcoE - TRILL-Dual PSU - Dual Fan; 01 thiết bị tường lửa ASA 5525-X with FirePOWER Svcs. Chassis and Subs. Bundle, 01 bộ định tuyến, 01 CoreSwitch - FF 5700, 01 tủ PDU, WinSvrSTDCore 2019, Hệ thống chữa cháy tự động FM 200, 02 máy lạnh chính xác, hệ thống camera giám sát, hệ thống lưu điện, tủ Rack… cơ bản đã đáp ứng việc triển khai các ứng dụng CNTT phục vụ các cơ quan đảng.

2. Sự cần thiết thuê dịch vụ công nghệ thông tin đối với Giải pháp đảm bảo an toàn thông tin cho hệ thống CNTT tại Trung tâm tích hợp dữ liệu của Tỉnh ủy

2.1. Đối với việc lựa chọn hình thức thuê Dịch vụ công nghệ thông tin:

Mục đích của việc thuê dịch vụ CNTT là nhằm tối ưu hóa chi phí, tận dụng nguồn nhân lực của các nhà cung cấp dịch vụ CNTT bù đắp thiếu hụt về nhân lực CNTT của tổ chức, đơn vị để nâng cao chất lượng hệ thống CNTT, đạt được một mức độ an toàn và sẵn sàng cao hơn của hệ thống, cũng như khả năng tập trung phát huy những mặt mạnh của tổ chức.

Lợi ích thuê dịch vụ CNTT:

- Linh hoạt và tiếp cận công nghệ mới: Các nhà cung cấp công nghệ hàng đầu luôn theo kịp với những thay đổi và cải tiến mới nhất trong lĩnh vực công nghệ. Do vậy, khi thuê dịch vụ CNTT từ các nhà cung cấp dịch vụ các đơn vị, tổ chức sẽ được áp dụng những công nghệ mới giúp tăng hiệu quả và độ tin cậy cho hệ thống CNTT của mình. Hơn nữa, khi thuê ngoài dịch vụ CNTT, tùy thuộc vào nhu cầu thực tế các đơn vị, tổ chức có thể thu hẹp hay mở rộng nhanh chóng tài nguyên, dịch vụ một cách dễ dàng và thuận tiện nếu muốn.

- Tiết kiệm chi phí: Khi thuê dịch vụ CNTT đơn vị tổ chức sẽ giảm được chi phí đầu tư hạ tầng CNTT ban đầu, chi phí nhân sự quản trị, vận hành hệ thống.

- Lợi ích về chất lượng dịch vụ: Nhà cung cấp dịch vụ CNTT là đơn vị chuyên nghiệp về CNTT nên có hệ thống đào tạo bài bản cho nhân viên, cũng như các phòng thí nghiệm để thử nghiệm giải pháp trước khi đưa ra cho khách hàng. Họ cũng có các hệ thống giám sát về chất lượng công việc của nhân viên và đảm bảo quy trình dịch vụ. Các dịch vụ họ cung cấp do đó có tính chuyên nghiệp cao. Với việc đảm bảo về số lượng và chất lượng nguồn nhân lực CNTT của nhà cung cấp dịch vụ, các dịch vụ CNTT phục vụ cho hoạt động của cơ quan, tổ chức sẽ được nâng cao và đảm bảo chất lượng.

2.2. Đối với Dịch vụ Giải pháp đảm bảo an toàn thông tin cho hệ thống CNTT tại Trung tâm tích hợp dữ liệu của các cơ quan Đảng

Nhận thức được tầm quan trọng của ATTT nên Đảng, Nhà nước đã chỉ đạo các bộ/ngành, địa phương triển khai xây dựng nhiều chủ trương, chính sách về ATTT. Bộ Thông tin và Truyền thông (TT&TT) với trách nhiệm quản lý nhà nước trong lĩnh vực ATTT đã phối hợp với các bộ/ngành xây dựng, hoàn thiện nhiều hệ thống các văn bản quy phạm pháp luật về ATTT.

- Luật ATTT mạng được ban hành năm 2015 đã thể chế hóa các chủ trương, đường lối, chính sách của Đảng và Nhà nước về ATTT, đáp ứng yêu cầu phát triển bền vững kinh tế - xã hội, bảo vệ thông tin và hệ thống thông tin, góp phần bảo đảm quốc phòng, an ninh, chủ quyền và lợi ích quốc gia trên không gian mạng.

- Ngày 01/07/2016, Chính phủ đã ban hành Nghị định số 85/2016/NĐ-CP Về bảo đảm an toàn hệ thống thông tin theo cấp độ.

- Ngày 24/4/2017, Bộ Thông tin và Truyền thông ban hành Thông tư số 03/2017/TT-BTTTT 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.

- Ngày 25/9/2017, Bộ trưởng Bộ Khoa học và Công nghệ ban hành Quyết định số 2582/QĐ-BKHCN về việc công bố Tiêu chuẩn quốc gia TCVN - 11930:2017 yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ.

- Ngày 25/05/2018, Thủ tướng Chính phủ có Chỉ thị số 14/CT-TTg về việc nâng cao năng lực phòng, chống phần mềm độc hại.

- Ngày 07/06/2019, Thủ tướng Chính phủ có Chỉ thị số 14/CT-TTg về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam.

- Ngày 04/09/2019 của Bộ Thông tin và Truyền thông ban hành Công văn số 2973/BTTTT-CATTT về việc "Hướng dẫn triển khai hoạt động giám sát an toàn thông tin trong cơ quan, tổ chức nhà nước".

- Ngày 08 tháng 04 năm 2020, Bộ Thông tin và Truyền thông ban hành Công văn số 235/CATTT-ATHTTT về Hướng dẫn Mô hình đảm bảo an toàn thông tin cấp Bộ, Tỉnh (mô hình 4 lớp).

- Chỉ thị số 41/CT-TW ngày 24/3/2020 và Công văn số 1552/BTTTT-CATTT ngày 28/4/2020 yêu cầu mỗi cơ quan Đảng, Nhà nước triển khai công tác an toàn, an ninh mạng đồng bộ, theo mô hình "4 lớp" bao gồm: Kiện toàn lực lượng tại chỗ; Lựa chọn tối thiểu một tổ chức, doanh nghiệp giám sát, bảo vệ chuyên nghiệp; Định kỳ thực hiện kiểm tra, đánh giá độc lập; Kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia.

Các Nghị quyết, Chỉ thị của Đảng, cũng như các văn bản quy phạm pháp luật của Nhà nước đều thống nhất quan điểm chỉ đạo về bảo đảm an toàn, an ninh thông tin và bảo vệ chủ quyền quốc gia trên không gian mạng.

Từ các căn cứ pháp lý trên và việc đánh giá hiện trạng ATTT tại Trung tâm tích hợp dữ liệu của các cơ quan Đảng cho thấy nguy cơ mất ATTT là hiện hữu. Do vậy việc thuê dịch vụ đảm bảo an toàn thông tin cho hệ thống CNTT tại Trung tâm tích hợp dữ liệu của các cơ quan Đảng là thực sự cần thiết, phù hợp với định hướng và theo quy định của Pháp luật, hướng dẫn của Bộ TTTT nhằm tăng cường đảm bảo an toàn thông tin mạng, nhằm góp phần đẩy mạnh thực hiện Chương trình chuyển đổi số tỉnh Đồng Nai. Đặc biệt là trong bối cảnh xây dựng và thực hiện Chính phủ điện tử, hướng tới Chính phủ số và một nền kinh tế số. Nghị quyết số 52-NQ/TW ngày 27/9/2019 của Bộ Chính trị về một số chủ trương chính sách chủ động tham gia cuộc Cách mạng công nghiệp lần thứ tư đã nhấn mạnh việc thúc đẩy chuyển đổi số trong các cơ quan Đảng, Nhà nước, Mặt trận và các tổ chức chính trị xã hội.

II. NỘI DUNG THUÊ DỊCH VỤ CÔNG NGHỆ THÔNG TIN

1. Tên nhiệm vụ: Kế hoạch thuê Dịch vụ công nghệ thông tin Giải pháp đảm bảo an toàn thông tin cho hệ thống CNTT tại Trung tâm tích hợp dữ liệu của Tỉnh ủy.

2. Mục tiêu:

- Đảm bảo ATTT cho hoạt động truy cập, khai thác, sử dụng các hệ thống thông tin và cơ sở dữ liệu trên hệ thống thông tin có kết nối mạng Internet của Trung tâm tích hợp dữ liệu các cơ quan Đảng Tỉnh Ủy Đồng Nai.

- Triển khai dịch vụ giám sát an toàn thông tin mạng 24/7 cho cho hệ thống công nghệ thông tin Trung tâm tích hợp dữ liệu các cơ quan Đảng nhằm:

+ Tăng cường năng lực kết nối giám sát và thu thập các sự kiện về an toàn thông tin trên các hệ thống CNTT quan trọng hiện hữu của tỉnh, nhằm đưa ra được bức tranh tổng thể về an toàn thông tin trong thời gian thực.

+ Có khả năng thực hiện công tác cảnh báo phát hiện các sự cố về an toàn thông tin nhằm kịp thời ngăn chặn và hoặc xử lý rủi ro.

+ Cung cấp và hỗ trợ các đơn vị trong việc đánh giá định kỳ về an toàn thông tin.

+ Bước đầu xây dựng quy trình và đáp ứng nhu cầu nâng cao khả năng tiếp nhận thông tin và quản lý, chỉ huy điều hành công tác CNTT và ứng cứu an toàn thông tin trên địa bàn tỉnh.

+ Thực hiện công tác quản lý nhà nước trong lĩnh vực thông tin điện tử, xử phạt hành chính, truy vết các sai phạm trong an toàn, an ninh thông tin.

+ Phòng ngừa những hư hỏng có thể xảy ra trong quá trình vận hành hệ thống CNTT trọng yếu của tỉnh liên tục 24/7.

+ Tăng cường an toàn, an ninh thông tin mạng cho các cơ quan Đảng trên địa bàn tỉnh; các hệ thống thông tin trọng yếu của tỉnh nhằm tránh tình trạng lộ lọt thông tin.

+ Phát hiện các dấu hiệu về hành vi bất thường, các sự cố mất an toàn thông tin và các nguy cơ xảy ra sự cố mất an toàn thông tin.

+ Cảnh báo về các hành vi bất thường, các sự cố mất an toàn thông tin và các nguy cơ xảy ra sự cố mất an toàn thông tin.

+ Điều tra bổ sung thông tin nhằm xác định mức độ chính xác, mức độ ảnh hưởng, các thông tin liên quan được sử dụng trong việc phản ứng với sự cố mất an toàn thông tin.

+ Phản ứng lại các sự cố mất an toàn thông tin, kịp thời ngăn chặn, giảm thiểu và khắc phục các rủi ro gây ra bởi sự cố mất an toàn thông tin.

+ Xây dựng hệ thống điều hành tập trung để bao quát được các vấn đề về an toàn thông tin cho các cơ quan Đảng trên địa bàn tỉnh cũng như phản ứng nhanh

với các tấn công mạng một cách tập trung, xóa bỏ khoảng cách về mặt địa lý.

3. Nội dung thuê: Giải pháp đảm bảo an toàn thông tin cho hệ thống Công nghệ thông tin tại Trung tâm tích hợp dữ liệu của Tỉnh ủy.

STT	Danh mục	Thời gian thực hiện hợp đồng (năm)	ĐVT	Số lượng
I	**Dịch vụ giám sát ATTT 24/7**			
	Dịch vụ giám sát An toàn thông tin mạng cho hệ thống CNTT tại TTTHDL của các cơ quan Đảng quy mô 35 máy chủ. Các tính năng bao gồm: Giám sát, cảnh báo ATTT 24/7: - Giám sát ATTT Endpoint: Phát hiện thiết bị đầu cuối nhiễm mã độc APT. - Giám sát ATTT lớp mạng: Phát hiện kết nối C&C trong phân vùng mạng có máy chủ cần giám sát; Phát hiện Shellcode/payload tấn công trong traffic mạng thuộc phân vùng mạng có máy chủ cần giám sát; - Giám sát ATTT ứng dụng. - Điều tra, xác minh sự kiện: Điều tra, xác minh sự kiện ATTT từ xa; Tối ưu ATTT: - Bổ sung rule/usecase phát hiện kỹ thuật tấn công mới định kỳ - Tối ưu rule/usecase phát sinh nhiều cảnh báo sai định kỳ. Báo cáo ATTT: - Tình hình vận hành, giám sát hàng tháng; - Báo cáo xử lý sự cố (nếu có). Hỗ trợ xử lý sự cố ATTT: - Lấy mẫu, phân tích mã độc webshell; - Điều tra tấn công xâm nhập, tấn công APT; - Phản ứng: chặn điều khiển, làm sạch.	3	Gói	1
II	**Dịch vụ thuê giải pháp phần mềm**			
1	**Phần mềm điều phối, tự động hóa và phản ứng an ninh mạng SOAR:**	3	License	1

STT	Danh mục	Thời gian thực hiện hợp đồng (năm)	ĐVT	Số lượng
	- Tự động thu thập cảnh báo và sự kiện từ SIEM; - Phân loại mức độ ưu tiên của cảnh báo - Tự động tạo sự cố (incident) - Thu thập và quản lý bằng chứng cho sự cố - Đồ thị quan hệ trực quan các đối tượng liên quan trong sự cố - Lập lịch và xuất báo cáo qua giao diện trực quan - Quản lý ticket xử lý, gán đơn vị/người xử lý theo tổ chức - Định nghĩa các thỏa thuận mức dịch vụ (service-level agreement - SLA) phù hợp với tính chất của tổ chức, tính chất của yêu cầu - Thông báo ticket mới, ticket sắp hết hạn - Thống kê chỉ số đánh giá thực hiện công việc (Key Performance Indicator - KPI) ticket xử lý theo từng đơn vị; - Hỗ trợ đồ thị quan hệ trực quan các đối tượng liên quan đến sự cố. - Cung cấp tính năng ticketing builtin.			
2	**Phần mềm giám sát an ninh mạng SIEM:** - Khả năng cảnh báo thời gian thực (Real Time Alert) cho phép gửi thông tin cảnh báo thời gian thực từ hệ thống ngay khi có sự cố xảy ra. - Agent thu thập Log trên Windows; Agent thu thập Log trên Linux; Thu thập Windows Event; Thu thập Log qua Syslog. - Cung cấp sẵn các bộ chuẩn hóa Log. - Tìm kiếm nhanh Alert, Trích xuất kết quả tìm kiếm - Dashboard & Report: Cung cấp sẵn các biểu đồ, báo cáo phổ biến; Cho phép người dùng định nghĩa báo cáo từ các biểu đồ có sẵn; Gửi báo cáo định kỳ qua Email; Báo cáo trích xuất ra file.	3	License	1

STT	Danh mục	Thời gian thực hiện hợp đồng (năm)	ĐVT	Số lượng
	- Thêm mhanh điều kiện tìm kiếm từ giao diện. - Tạo các biểu đồ thống kê dữ liệu. - Phân tích tương quan sự kiện nhật ký theo thời gian thực. - Tạo báo cáo theo các mẫu đã được định nghĩa qua giao diện đồ họa. - Kết nối chia sẻ thông tin giám sát với Trung Tâm Giám Sát An Toàn Không Gian Mạng Quốc Gia - NCSC			
3	**Dịch vụ phần mềm giám sát bất thường và phát hiện tấn công có chủ đích ở lớp mạng:** - Phát hiện tấn công rà quét mật khẩu trong mạng. - Phát hiện dấu hiệu tấn công từ chối dịch vụ. - Phát hiện dấu hiệu tấn công rà quét lỗ hổng. - Phát hiện dấu hiệu tấn công ứng dụng Web (SQL Injection, XSS,…) - Phát hiện các dấu hiệu IoC của mã độc APT - Phát hiện các kỹ thuật tấn công theo khung MITRE ATT&CK - Phát hiện dấu hiệu rà quét thông tin mạng. - Phát hiện dấu hiệu khai thác dịch vụ.	3	License	1
4	**Phần mềm giám sát, phát hiện tấn công có chủ đích (EDR) cho tối đa 35 máy chủ:** - Giám sát các hành vi ở mức nhân hệ điều hành trên hệ điều hành: Máy chủ (Windows Server 2008R2 trở lên; CentOS 7, Ubuntu 18). - Phân tích hành vi và xử lý tập trung. - Theo dõi tình hình cài đặt, trạng thái hoạt động của máy chủ - Cảnh báo kịp thời các bất thường phát hiện trên máy chủ. - Phát hiện dấu hiệu tấn công nâng cao APT theo MITRE ATT&CK	3	License	1

STT	Danh mục	Thời gian thực hiện hợp đồng (năm)	ĐVT	Số lượng
	- Cung cấp giao diện khép kín điều tra các cuộc tấn công (IR Flow): Detection - Investigation - Response. - Hỗ trợ cô lập (network, process) tạm thời các máy phục vụ điều tra.			

4. Mô tả dịch vụ

Các dịch vụ, giải pháp phải tuân thủ các quy định hoạt động giám sát an toàn hệ thống thông tin tại Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông.

Đáp ứng các yêu cầu theo hướng dẫn của cơ quan chức năng (tại văn bản số 2973/BTTTT-CATTT ngày 04/09/2019 của BTTTT về việc hướng dẫn triển khai hoạt động giám sát an toàn thông tin trong cơ quan, tổ chức nhà nước và Văn bản số 235/CATTT ATHTTT ngày 08/04/2020 của Cục An toàn thông tin về việc hướng dẫn mô hình đảm bảo an toàn thông tin cấp bộ, tỉnh) về mô hình giám sát an toàn thông tin cho cấp tỉnh.

Đảm bảo đáp ứng tiêu chí về Chất lượng dịch vụ theo Quyết định số 1356/QĐ-BTTTT ngày 07/7/2022 của Bộ Thông tin và Truyền thông ban hành Tiêu chí đánh giá giải pháp, dịch vụ Trung tâm giám sát điều hành an toàn, an ninh mạng (SOC).

Gồm các dịch vụ sau:

- Dịch vụ giám sát, xử lý sự cố an toàn thông tin mạng 24/7 cho hệ thống CNTT trong Trung tâm tích hợp dữ liệu các cơ quan Đảng với quy mô tối đa 35 máy chủ.
- Phần mềm điều phối, tự động hóa và phản ứng an ninh mạng SOAR.
- Phần mềm giám sát an ninh mạng SIEM.
- Phần mềm giám sát bất thường và phát hiện tấn công có chủ đích ở lớp mạng.
- Phần mềm giám sát, phát hiện tấn công có chủ đích (EDR) cho tối đa 35 máy chủ.

5. Khái toán đầu tư

Tổng mức đầu tư: 4.500.000.000 đồng (Bốn tỷ năm trăm triệu đồng)

Trong đó:

TT	Nội dung	Dự toán kinh phí	Ký hiệu
I	Chi phí thuê dịch vụ	4.256.812.838	Gdv
II	Chi phí quản lý dự án	117.330.675	Gql
III	Chi phí tư vấn	95.431.021	Gtv
IV	Chi phí khác	30.425.466	Gk
V	Chi phí dự phòng	-	Gdp
	TỔNG CỘNG	**4.500.000.000**	Gt

(Chi tiết trong Phụ lục đính kèm)

6. Nguồn kinh phí thực hiện: Vốn sự nghiệp ngân sách tỉnh.

7. Thời gian thuê: 03 năm, tính từ thời điểm ký hợp đồng thuê *(không tính thời gian thực hiện thủ tục).*

Văn phòng Tỉnh ủy kính trình Ủy ban nhân dân tỉnh xem xét chấp thuận chủ trương thuê Dịch vụ công nghệ thông tin Giải pháp đảm bảo an toàn thông tin cho hệ thống Công nghệ thông tin tại Trung tâm tích hợp dữ liệu của Tỉnh ủy theo quy định.

Nơi nhận:
- Như trên,
- TTTU (b/c),
- Sở: Tài chính, Thông tin và truyền thông,
- CP.VPTU,
- Phòng TC, HC-QT, CY-CNTT (MT),
- Lưu VPTU.

K/T CHÁNH VĂN PHÒNG
PHÓ CHÁNH VĂN PHÒNG

[]
Nguyễn Xuân Cường

PHỤ LỤC 1

BẢNG TỔNG DỰ TOÁN

STT	Nội dung chi phí	Diễn giải		Giá trị trước thuế	Thuế GTGT	Giá trị sau thuế	Ghi chú
I	**Chi phí thuê dịch vụ**	**Gdv**		**4.034.200.071**	**222.612.767**	**4.256.812.838**	
1	**Chi phí thuê dịch vụ/phần mềm có sẵn trên thị trường**			**4.034.200.071**	**222.612.767**	**4.256.812.838**	
	Giải pháp đảm bảo an toàn thông tin cho hệ thống CNTT tại Trung tâm tích hợp dữ liệu của các cơ quan Đảng	**Gdvm**	Theo báo giá thị trường	4.034.200.071	222.612.767	4.256.812.838	
II	**Chi phí quản lý kế hoạch thuê**	**Gql**		**106.664.250**	**10.666.425**	**117.330.675**	
1	**Chi phí thực hiện quản lý Kế hoạch thuê**	**Gqlkht**		**106.664.250**	**10.666.425**	**117.330.675**	Bảng số 1 - QĐ số 1688/QĐ-BTTTT
	Hạng mục hạ tầng kỹ thuật CNTT	2,644 %	x Gdv	106.664.250	10.666.425	117.330.675	
III	**Chi phí tư vấn đầu tư**	**Gtv**	**III= 1+2+3+4**	**86.755.473**	**8.675.548**	**95.431.021**	
1	**Lập Kế hoạch thuê**			**40.019.265**	**4.001.927**	**44.021.192**	Bảng số 2 - QĐ số 1688/QĐ-BTTTT
	Hạng mục hạ tầng kỹ thuật CNTT	0,992 %	x Gdv	40.019.265	4.001.927	44.021.192	
2	**Chi phí thẩm tra**			**6.353.865**	**635.386**	**6.989.251**	

STT	Nội dung chi phí	Diễn giải		Giá trị trước thuế	Thuế GTGT	Giá trị sau thuế	Ghi chú
2.1	*Chi phí thẩm tra tính hiệu quả và tính khả thi của dự án đầu tư*			*1.694.364*	*169.436*	*1.863.800*	*Bảng số 4 - QĐ số 1688/QĐ-BTTTT*
	Hạng mục hạ tầng kỹ thuật CNTT	0,105 %	x Gdv x40%	1.694.364	169.436	1.863.800	
2.2	*Chi phí thẩm tra thiết kế thi công*			*2.456.828*	*245.683*	*2.702.511*	*Bảng số 5 - QĐ số 1688/QĐ-BTTTT*
	Hạng mục hạ tầng kỹ thuật CNTT	0,087 %	x Gdv x70%	2.456.828	245.683	2.702.511	
2.3	*Chi phí thẩm tra dự toán*			*2.202.673*	*220.267*	*2.422.940*	*Bảng số 6 - QĐ số 1688/QĐ-BTTTT*
	Hạng mục hạ tầng kỹ thuật CNTT	0,078 %	x Gdv x70%	2.202.673	220.267	2.422.940	
3	**Chi phí lập hồ sơ mời thầu, đánh giá hồ sơ dự thầu**			**11.416.786**	**1.141.679**	**12.558.465**	Bảng số 8 - QĐ số 1688/QĐ-BTTTT
	Hạng mục hạ tầng kỹ thuật CNTT	0,283 %	x Gdv	11.416.786	1.141.679	12.558.465	
4	**Chi phí giám sát**			**28.965.557**	**2.896.556**	**31.862.113**	Bảng số 9 - QĐ số

STT	Nội dung chi phí	Diễn giải		Giá trị trước thuế	Thuế GTGT	Giá trị sau thuế	Ghi chú
							1688/QĐ-BTTTT
	Hạng mục hạ tầng kỹ thuật CNTT	0,718 %	x Gdv	28.965.557	2.896.556	31.862.113	
IV	**Chi phí khác có liên quan**	**Gk**		**27.659.515**	**2.765.951**	**30.425.466**	
1	Chi phí thẩm định Hồ sơ mời thầu	0,050 %	x Gdv	2.017.100	201.710	2.218.810	Nghị định 63/2014/NĐ-CP
2	Chi phí thẩm định kết quả lựa chọn nhà thầu	0,050 %	x Gdv	2.017.100	201.710	2.218.810	Nghị định 63/2014/NĐ-CP
3	Chi phí thẩm định giá	0,555 %	x Gdv sau VAT	23.625.315	2.362.531	25.987.846	Tạm tính
V	**Chi phí dự phòng**	**Gdp**		**-**	**-**	**-**	
1	Chi phí dự phòng	0%		-	-	-	
	Tổng cộng	**Gt**	**I + II + III + IV + V**	**4.255.279.309**	**244.720.691**	**4.500.000.000**	

PHỤ LỤC 2: CHI PHÍ THUÊ DỊCH VỤ CÔNG NGHỆ THÔNG TIN
Giải pháp đảm bảo an toàn thông tin cho hệ thống Công nghệ thông tin tại Trung tâm tích hợp dữ liệu của Tỉnh ủy

STT	Danh mục	Thời gian thực hiện hợp đồng (năm)	ĐVT	Số lượng	Giá trị trước thuế		Thuế VAT		Tổng cộng
					Đơn giá	Thành tiền	%	Thành tiền	
I	**Dịch vụ giám sát ATTT 24/7**								
	Dịch vụ giám sát An toàn thông tin mạng cho hệ thống CNTT tại TTDL của Tỉnh Ủy quy mô 35 máy chủ. Các tính năng bao gồm: Giám sát, cảnh báo ATTT 24/7: - Giám sát ATTT Endpoint: Phát hiện thiết bị đầu cuối nhiễm mã độc APT. - Giám sát ATTT lớp mạng: Phát hiện kết nối C&C trong phân vùng mạng có máy chủ cần giám sát; Phát hiện Shellcode/payload tấn công trong traffic mạng	3	Gói	1	602.690.800	1.808.072.400	-	-	1.808.072.400

STT	Danh mục	Thời gian thực hiện hợp đồng (năm)	ĐVT	Số lượng	Giá trị trước thuế		Thuế VAT		Tổng cộng
					Đơn giá	Thành tiền	%	Thành tiền	
	thuộc phân vùng mạng có máy chủ cần giám sát; - Giám sát ATTT ứng dụng. - Điều tra, xác minh sự kiện: Điều tra, xác minh sự kiện ATTT từ xa; Tối ưu ATTT: - Bổ sung rule/usecase phát hiện kỹ thuật tấn công mới định kỳ - Tối ưu rule/usecase phát sinh nhiều cảnh báo sai định kỳ. Báo cáo ATTT: - Tình hình vận hành, giám sát hàng tháng; - Báo cáo xử lý sự cố (nếu có). Hỗ trợ xử lý sự cố ATTT: - Lấy mẫu, phân tích mã độc webshell; - Điều tra tấn công xâm nhập, tấn công APT; - Phản ứng: chặn điều khiển, làm sạch.								

STT	Danh mục	Thời gian thực hiện hợp đồng (năm)	ĐVT	Số lượng	Giá trị trước thuế		Thuế VAT		Tổng cộng
					Đơn giá	Thành tiền	%	Thành tiền	
II	**Dịch vụ thuê giải pháp phần mềm**								
1	**Phần mềm điều phối, tự động hóa và phản ứng an ninh mạng SOAR:** - Tự động thu thập cảnh báo và sự kiện từ SIEM; - Phân loại mức độ ưu tiên của cảnh báo - Tự động tạo sự cố (incident) - Thu thập và quản lý bằng chứng cho sự cố - Đồ thị quan hệ trực quan các đối tượng liên quan trong sự cố - Lập lịch và xuất báo cáo qua giao diện trực quan - Quản lý ticket xử lý, gán đơn vị/người xử lý theo tổ chức - Định nghĩa các thỏa thuận mức dịch vụ (service-level agreement – SLA) phù hợp với tính chất của tổ chức,	3	License	1	214.288.557	642.865.671	10%	64.286.567	707.152.238

STT	Danh mục	Thời gian thực hiện hợp đồng (năm)	ĐVT	Số lượng	Giá trị trước thuế		Thuế VAT		Tổng cộng
					Đơn giá	Thành tiền	%	Thành tiền	
	tính chất của yêu cầu - Thông báo ticket mới, ticket sắp hết hạn - Thống kê chỉ số đánh giá thực hiện công việc (Key Performance Indicator – KPI) ticket xử lý theo từng đơn vị; - Hỗ trợ đồ thị quan hệ trực quan các đối tượng liên quan đến sự cố. - Cung cấp tính năng ticketing builtin.								
2	**Phần mềm giám sát an ninh mạng SIEM:** - Khả năng cảnh báo thời gian thực (Real Time Alert) cho phép gửi thông tin cảnh báo thời gian thực từ hệ thống ngay khi có sự cố xảy ra. - Agent thu thập Log trên Windows; Agent thu thập Log trên Linux; Thu thập Windows Event; Thu thập	3	License	1	300.182.000	900.546.000	0	90.054.600	990.600.600

STT	Danh mục	Thời gian thực hiện hợp đồng (năm)	ĐVT	Số lượng	Giá trị trước thuế		Thuế VAT		Tổng cộng
					Đơn giá	Thành tiền	%	Thành tiền	
	Log qua Syslog. - Cung cấp sẵn các bộ chuẩn hóa Log. - Tìm kiếm nhanh Alert, Trích xuất kết quả tìm kiếm - Dashboard & Report: Cung cấp sẵn các biểu đồ, báo cáo phổ biến; Cho phép người dùng định nghĩa báo cáo từ các biểu đồ có sẵn; Gửi báo cáo định kỳ qua Email; Báo cáo trích xuất ra file. - Thêm mhanh điều kiện tìm kiếm từ giao diện. - Tạo các biểu đồ thống kê dữ liệu. - Phân tích tương quan sự kiện nhật ký theo thời gian thực; - Tạo báo cáo theo các mẫu đã được định nghĩa qua giao diện đồ họa. - Kết nối chia sẻ thông tin giám sát với Trung Tâm								

STT	Danh mục	Thời gian thực hiện hợp đồng (năm)	ĐVT	Số lượng	Giá trị trước thuế		Thuế VAT		Tổng cộng
					Đơn giá	Thành tiền	%	Thành tiền	
	Giám Sát An Toàn Không Gian Mạng Quốc Gia - NCSC								
3	**Dịch vụ phần mềm giám sát bất thường và phát hiện tấn công có chủ đích ở lớp mạng:** - Phát hiện tấn công rà quét mật khẩu trong mạng. - Phát hiện dấu hiệu tấn công từ chối dịch vụ. - Phát hiện dấu hiệu tấn công rà quét lỗ hổng. - Phát hiện dấu hiệu tấn công ứng dụng Web (SQL Injection, XSS,…) - Phát hiện các dấu hiệu IoC của mã độc APT - Phát hiện các kỹ thuật tấn công theo khung MITRE ATT&CK - Phát hiện dấu hiệu rà quét thông tin mạng. - Phát hiện dấu hiệu khai thác dịch vụ.	3	License	1	156.762.000	470.286.000	10%	47.028.600	517.314.600

STT	Danh mục	Thời gian thực hiện hợp đồng (năm)	ĐVT	Số lượng	Giá trị trước thuế		Thuế VAT		Tổng cộng
					Đơn giá	Thành tiền	%	Thành tiền	
4	**Phần mềm giám sát, phát hiện tấn công có chủ đích (EDR) cho tối đa 35 máy chủ:** - Giám sát các hành vi ở mức nhân hệ điều hành trên hệ điều hành: Máy chủ (Windows Server 2008R2 trở lên; CentOS 7, Ubuntu 18). - Phân tích hành vi và xử lý tập trung. - Theo dõi tình hình cài đặt, trạng thái hoạt động của máy chủ - Cảnh báo kịp thời các bất thường phát hiện trên máy chủ. - Phát hiện dấu hiệu tấn công nâng cao APT theo MITRE ATT&CK - Cung cấp giao diện khép kín điều tra các cuộc tấn công (IR Flow): Detection – Investigation - Response.	3	License	1	70.810.000	212.430.000	10%	21.243.000	233.673.000

STT	Danh mục	Thời gian thực hiện hợp đồng (năm)	ĐVT	Số lượng	Giá trị trước thuế		Thuế VAT		Tổng cộng
					Đơn giá	Thành tiền	%	Thành tiền	
	- Hỗ trợ cô lập (network, process) tạm thời các máy phục vụ điều tra.								
	Tổng Cộng					**4.034.200.071**		**222.612.767**	**4.256.812.838**