UBND TỈNH KHÁNH HÒA
SỞ KHOA HỌC VÀ CÔNG NGHỆ

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 598 /KH-SKHCN

Khánh Hòa, ngày 12 tháng 4 năm 2023

KẾ HOẠCH

Ứng phó sự cố an toàn thông tin mạng của Sở Khoa học và Công nghệ năm 2023

Thực hiện Kế hoạch số 2517/KH-UBND ngày 17/3/2023 của Ủy ban nhân dân tỉnh về Ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Khánh Hòa năm 2023. Sở Khoa học và Công nghệ xây dựng Kế hoạch ứng phó sự cố, bảo đảm an toàn thông tin mạng của Sở năm 2023 như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích:

- Đảm bảo an toàn thông tin cho các hệ thống thông tin của Sở Khoa học và Công nghệ đảm bảo khả năng thích ứng một cách chủ động, linh hoạt và giảm thiểu các nguy cơ, đe dọa mất an toàn thông tin trên mạng, đề ra các giải pháp ứng phó khi gặp sự cố mất an toàn thông tin mạng.

- Nâng cao năng lực giám sát nhằm tăng cường khả năng phát hiện sớm, cảnh báo kịp thời, chính xác về các sự kiện, rủi ro, dấu hiệu, hành vi, mức độ xâm hại, nguy cơ, điểm yếu, lỗ hổng gây mất an toàn thông tin mạng đối với hệ thống, dịch vụ công nghệ thông tin phục vụ chính phủ điện tử của Sở.

- Đảm bảo các nguồn lực và các điều kiện cần thiết để sẵn sàng triển khai kịp thời, hiệu quả các phương án ứng cứu khẩn cấp sự cố an toàn thông tin mạng.

2. Yêu cầu:

- Có phương án đối phó, ứng cứu sự cố an toàn thông tin mạng phải đặt ra được các tiêu chí để có thể nhanh chóng xác định được tính chất, mức độ nghiêm trọng khi sự cố xảy ra và đưa ra phương án xử lý kịp thời.

- Xác định cụ thể các nguồn lực đảm bảo, giải pháp tổ chức thực hiện và kinh phí để triển khai các nội dung của Kế hoạch, đảm bảo khả thi, hiệu quả.

- Thường xuyên trao đổi thông tin, chia sẻ kinh nghiệm trong công tác đảm bảo an toàn thông tin giữa Sở với các cơ quan nhà nước trên địa bàn tỉnh; giữa Sở với các đơn vị trực thuộc Sở và sự phối hợp, hỗ trợ của các đơn vị nghiệp vụ của Bộ Thông tin và Truyền thông.

II. NHIỆM VỤ TRIỂN KHAI

1. Triển khai các nhiệm vụ khi chưa có sự cố xảy ra:

a) Tuyên truyền, phổ biến các văn bản quy phạm pháp luật, tài liệu hướng dẫn chuyên môn về an toàn thông tin mạng.

- Nội dung thực hiện:

Tổ chức tuyên truyền, phổ biến, hướng dẫn nội dung của Luật An toàn thông tin mạng; Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ; Quyết định số 1017/QĐ-TTg ngày 14/8/2018 của Thủ tướng Chính phủ; Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Thủ tướng Chính phủ; Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông; Chỉ thị số 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ; Chỉ thị số 23/CT-TTg ngày 26/12/2022 của Thủ tướng Chính phủ; Kế hoạch số 13784/KH-UBND ngày 31/12/2020 của UBND tỉnh Khánh Hòa và các văn bản quy phạm pháp luật, tài liệu hướng dẫn chuyên môn về an toàn thông tin mạng trên các phương tiện thông tin đại chúng, trên Cổng Thông tin điện tử của tỉnh, Trang thông tin điện tử của Sở Khoa học và Công nghệ

- Đơn vị thực hiện: Vănphòng sở, các đơn vị thuộc Sở.

- Đơn vị phối hợp: Sở Thông tin và Truyền thông.

- Thời gian thực hiện: Thường xuyên trong năm.

b) Triển khai phòng ngừa sự cố, giám sát phát hiện sớm sự cố

- Nội dung thực hiện: Giám sát, phát hiện sớm các nguy cơ, sự cố; kiểm tra, đánh giá an toàn thông tin mạng và rà quét, bóc gỡ, phân tích, xử lý mã độc; phòng ngừa sự cố, quản lý rủi ro; nghiên cứu, phân tích, xác minh, cảnh báo sự cố, rủi ro an toàn thông tin mạng, phần mềm độc hại; xây dựng, áp dụng quy trình, quy định, tiêu chuẩn an toàn thông tin; tuyên truyền, nâng cao nhận thức về nguy cơ, sự cố, tấn công mạng.

- Đơn vị thực hiện: Văn phòng Sở

- Đơn vị phối hợp: Cơ quan điều phối quốc gia *(Trung tâm ứng cứu khẩn cấp máy tính Việt Nam – VNCERT),* Sở Thông tin và Truyền thông, đơn vị liên quan khác.

- Thời gian thực hiện: Định kỳ hàng quý.

c) Triển khai các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố

- Nội dung thực hiện: Trang bị, nâng cấp trang thiết bị, công cụ, phương tiện, gia hạn bản quyền phần mềm phục vụ ứng cứu, khắc phục sự cố; chuẩn bị các điều kiện bảo đảm, dự phòng các nguồn lực và tài chính để sẵn sàng đối phó, ứng cứu, khắc phục khi sự cố xảy ra.

- Đơn vị thực hiện: Văn phòng Sở.

- Đơn vị phối hợp: Cơ quan điều phối quốc gia *(Trung tâm ứng cứu khẩn cấp máy tính Việt Nam - VNCERT*), Sở Thông tin và Truyền thông, đơn vị liên quan khác.

- Thời gian thực hiện: định kỳ 6 tháng.

d) Đánh giá các nguy cơ, sự cố an toàn thông tin mạng

- Nội dung thực hiện: Tổ chức đánh giá hiện trạng và khả năng bảo đảm an toàn thông tin mạng của các hệ thống thông tin; đánh giá, dự báo các nguy

cơ, sự cố tấn công mạng có thể xảy ra với các hệ thống thông tin; đánh giá, dự báo các hậu quả, thiệt hại, tác động có thể nếu có xảy ra sự cố; đánh giá về hiện trạng phương tiện, trang thiết bị, công cụ hỗ trợ, nhân lực, vật lực phục vụ đối phó, ứng cứu, khắc phục sự cố.

- Đơn vị thực hiện: Văn phòng Sở.

- Đơn vị phối hợp: Sở Thông tin và Truyền thông, đơn vị cung cấp dịch vụ mạng.

- Thời gian thực hiện: Kiểm tra hệ thống thông tin định kỳ 06 tháng/01 lần.

đ) Xây dựng phương án đối phó, ứng cứu sự cố

Việc xây dựng phương án đối phó, ứng cứu sự cố cần đảm bảo các nội dung sau:

- Xác định nhanh chóng, kịp thời nguyên nhân nguồn gốc sự cố nhằm áp dụng phương án đối phó, ứng cứu, khắc phục sự cố phù hợp, trong đó lưu ý các sự cố sau: do bị tấn công mạng; do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật hoặc do lỗi đường điện, đường truyền, hosting, do lỗi của người quản trị, vận hành hệ thống; liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn...

- Phương án đối phó, ứng cứu, khắc phục sự cố đối với một hoặc nhiều tình huống sau:

+ Về tình huống sự cố do bị tấn công mạng gồm: từ chối dịch vụ; giả mạo; sử dụng mã độc; truy cập trái phép, chiếm quyền điều khiển; thay đổi giao diện; mã hóa phần mềm, dữ liệu, thiết bị; phá hoại thông tin, dữ liệu, phần mềm; nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu; tổng hợp sử dụng kết hợp nhiều hình thức và các hình thức tấn công mạng khác.

+ Về tình huống do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật, bao gồm các sự cố sau: nguồn điện; đường kết nối Internet; do lỗi phần mềm, phần cứng, ứng dụng của hệ thống thông tin; liên quan đến quá tải hệ thống; khác do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật và do lỗi của người quản trị, vận hành hệ thống.

e) Triển khai các chương trình đào tạo, bồi dưỡng kỹ năng đánh giá, ứng phó sự cố

Nội dung thực hiện: Phối hợp với Sở Thông tin và Truyền thông tổ chức huấn luyện, diễn tập các phương án đối phó, ứng cứu sự cố tương ứng với các kịch bản, tình huống sự cố cụ thể; đào tạo nâng cao kỹ năng, nghiệp vụ phối hợp, ứng cứu, chống tấn công, xử lý mã độc, khắc phục sự cố; tham gia huấn luyện, đào tạo, bồi dưỡng, diễn tập vùng, miền, quốc gia.

- Đơn vị thực hiện: Văn phòng Sở.

- Đơn vị phối hợp: Sở Thông tin và Truyền thông, Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa và các đơn vị có liên quan.

2. Triển khai các nhiệm vụ khi có sự cố xảy ra: Thực hiện theo Quy trình ứng cứu, xử lý khẩn cấp sự cố tấn công mạng *(Phụ lục I đính kèm)*

III. KINH PHÍ THỰC HIỆN

Căn cứ Thông tư số 121/2018/TT-BTC ngày 12/12/2018 của Bộ trưởng Bộ Tài chính quy định về lập dự toán, quản lý, sử dụng và quyết toán kinh phí thực hiện công tác ứng cứu sự cố, đảm bảo an toàn thông tin.

Bảng dự toán kinh phí thực hiện đánh giá các nguy cơ, sự cố an toàn thông tin mạng cho hệ thống thông tin và đào tạo, huấn luyện ứng cứu sự cố an toàn thông tin mạng của Sở Khoa học và Công nghệ năm 2023 *(Phụ lục II đính kèm)*.

IV. TỔ CHỨC THỰC HIỆN

1. Văn phòng Sở

- Chủ trì, phối hợp với cơ quan, đơn vị liên quan tổ chức triển khai thực hiện tốt các nội dung nêu tại Kế hoạch này.

- Đôn đốc, theo dõi, tổng hợp và báo cáo các cơ quan liên quan về kết quả thực hiện.

2. Các đơn vị trực thuộc Sở

- Trên cơ sở Kế hoạch của Sở, các đơn vị trực thuộc căn cứ vào chức năng, nhiệm vụ được giao xây dựng Kế hoạch Ứng phó sự cố an toàn thông tin mạng để triển khai thực hiện.

- Báo cáo kết quả thực hiện gửi về Văn phòng sở để tổng hợp, báo cáo khi có yêu cầu.

Trong quá trình triển khai thực hiện Kế hoạch nếu khó khăn, vướng mắc báo cáo gửi về Văn phòng sở tổng hợp, đề nghị cơ quan liên quan hướng dẫn kịp thời./.

Nơi nhận:
- UBND tỉnh (báo cáo);
- Sở Tài chính;
- Sở Thông tin và Truyền thông;
- Các phòng, đơn vị (t/hiện);
- Lưu: VT, VP.

(VBĐT);

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ KHOA HỌC VÀ CÔNG NGHỆ
TỈNH KHÁNH HÒA

Lê Phước Đức

PHỤ LỤC I

QUY TRÌNH ỨNG CỨU, XỬ LÝ KHẨN CẤP SỰ CỐ TẤN CÔNG MẠNG

(Ban hành kèm theo Kế hoạch số 598 /KH-SKHCN ngày 12 /4/2023 của Sở Khoa học và Công nghệ)

Stt	Quy trình	Nội dung thực hiện	Đơn vị chủ trì	Đơn vị phối hợp
I	**Tiếp nhận, phân tích, ứng cứu ban đầu và thông báo sự cố**			
1.	Tiếp nhận, xác minh sự cố	Theo dõi, tiếp nhận, phân tích các cảnh báo, dấu hiệu sự cố có thể xảy ra từ các nguồn bên trong và bên ngoài. Khi phân tích, xác minh sự cố đã xảy ra, cần tổ chức ghi nhận, thu thập chứng cứ, xác định nguồn gốc sự cố.	Văn phòng Sở, Trung tâm Thông tin và Ứng dụng KHCN	Sở Thông tin và Truyền thông; Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa; Cơ quan điều phối quốc gia (Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam - VNCERT/CC).
2.	Triển khai các bước ưu tiên ứng cứu ban đầu	Căn cứ vào bản chất, dấu hiệu của sự cố tổ chức triển khai các bước ưu tiên ban đầu để xử lý sự cố theo Kế hoạch Ứng phó sự cố đã được cấp thẩm quyền phê duyệt hoặc theo hướng dẫn của Cơ quan chuyên trách ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh hoặc Cơ quan điều phối quốc gia.	Văn phòng Sở, Trung tâm Thông tin và Ứng dụng KHCN	Sở Thông tin và Truyền thông; Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa; Cơ quan điều phối quốc gia.
3.	Triển khai lựa chọn phương án ứng cứu	Căn cứ theo Kế hoạch Ứng phó sự cố đã được UBND tỉnh ban hành hoặc theo hướng dẫn của Cơ quan thường trực ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh để lựa chọn phương án ngăn chặn và xử lý sự cố; báo cáo, đề xuất Chủ quản hệ thống thông tin hoặc Ban Chỉ đạo chuyển đổi số tỉnh Khánh Hòa để xin ý kiến chỉ đạo (nếu cần thiết).	Văn phòng Sở, Trung tâm Thông tin và Ứng dụng KHCN	Sở Thông tin và Truyền thông; Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa; Cơ quan điều phối quốc gia.
4.	Chỉ đạo xử lý sự cố (trong trường hợp sự cố nghiêm trọng, cần triệu	Căn cứ theo báo cáo, đề xuất của Đơn vị quản lý, vận hành hệ thống thông tin, Ban Chỉ đạo Chuyển đổi số tỉnh Khánh Hòa phối hợp chủ quản hệ thống thông tin và tham khảo ý kiến Cơ quan điều phối quốc gia (nếu	Ban Chỉ đạo chuyển đổi số tỉnh Khánh Hòa	Đơn vị quản lý, vận hành hệ thống thông tin

	tập Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa và đề nghị Cơ quan điều phối quốc gia hỗ trợ)	cần) thực hiện chỉ đạo Cơ quan chuyên trách ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa triển khai công tác ứng cứu, xử lý.		
5.	Báo cáo sự cố	Sau khi đã triển khai các bước ưu tiên ứng cứu ban đầu, đơn vị quản lý, vận hành hệ thống thông tin tổ chức thông báo, báo cáo sự cố đến các tổ chức, cá nhân liên quan bên trong và bên ngoài cơ quan theo quy định tại Điều 9 Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc và quy định nội bộ (nếu có).	Văn phòng Sở, Trung tâm Thông tin và Ứng dụng KHCN	Sở Thông tin và Truyền thông; Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa; Cơ quan điều phối quốc gia.
6.	Điều phối công tác ứng cứu	Căn cứ vào tính chất sự cố, đề nghị hỗ trợ của đơn vị quản lý, vận hành hệ thống thông tin, Ban Chỉ đạo chuyển đổi số tỉnh Khánh Hòa, Cơ quan điều phối quốc gia hoặc Cơ quan chuyên trách ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh thực hiện công tác điều phối, giám sát cơ chế phối hợp, chia sẻ thông tin theo phạm vi, chức năng, nhiệm vụ của mình để huy động nguồn lực ứng cứu sự cố.	Ban Chỉ đạo chuyển đổi số tỉnh Khánh Hòa; Cơ quan điều phối quốc gia; Sở Thông tin và Truyền thông.	Sở Giáo dục và Đào tạo, Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa.
II	**Triển khai ứng cứu, ngăn chặn và xử lý sự cố**			
1	Triển khai ứng cứu, ngăn chặn và xử lý sự cố	Triển khai thu thập chứng cứ, phân tích, xác định phạm vi, đối tượng bị ảnh hưởng; phân tích, xác định nguồn gốc tấn công, tổ chức ứng cứu và ngăn chặn, giảm thiểu tác động, thiệt hại đến hệ thống thông tin.	Văn phòng Sở, Trung tâm Thông tin và Ứng dụng KHCN; Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng	Sở Thông tin và Truyền thông; Cơ quan điều phối quốc gia.

III	**Xử lý sự cố, gỡ bỏ, khôi phục và xử lý vi phạm**			
1.	Xử lý, gỡ bỏ sự cố	Sau khi đã triển khai ngăn chặn sự cố, đơn vị quản lý, vận hành hệ thống thông tin chịu trách nhiệm khẩn trương ngăn chặn sự cố, đồng thời tiêu diệt, gỡ bỏ các mã độc, phần mềm độc hại, khắc phục các điểm yếu an toàn thông tin của hệ thống thông tin (phối hợp với Sở Thông tin và Truyền thông và Đội ứng khẩn cấp sự cố an toàn thông tin mạng tỉnh nếu cần thiết).	Văn phòng Sở, Trung tâm Thông tin và Ứng dụng KHCN	Sở Thông tin và Truyền thông; Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa; Cơ quan điều phối quốc gia.
2.	Khôi phục sự cố	Đơn vị quản lý, vận hành hệ thống thông tin chủ trì phối hợp với các đơn vị liên quan triển khai các hoạt động khôi phục hệ thống thông tin, dữ liệu và kết nối; cấu hình hệ thống an toàn; bổ sung các thiết bị, phần cứng, phần mềm bảo đảm an toàn thông tin của hệ thống thông tin.	Văn phòng Sở, Trung tâm thông tin và Ứng dụng KHCN	Sở Thông tin và Truyền thông; Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa; Cơ quan điều phối quốc gia.
3.	Kiểm tra, đánh giá an toàn hệ thống thông tin sau khi khôi phục	Đơn vị quản lý, vận hành hệ thống thông tin và các đơn vị liên quan triển khai kiểm tra, đánh giá hoạt động của toàn bộ hệ thống thông tin sau khi khắc phục sự cố. Trường hợp hệ thống chưa đảm bảo an toàn, cần tiếp tục tổ chức thu thập, xác minh lại nguyên nhân và tổ chức ứng cứu để xử lý dứt điểm, khôi phục hoạt động của hệ thống thông tin trở lại bình thường.	Văn phòng Sở, Trung tâm Thông tin và Ứng dụng KHCN	Sở Thông tin và Truyền thông; Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa; Cục phòng chống tội phạm sử dụng công nghệ cao (Bộ Công an); Cơ quan điều phối quốc gia.
4.	Xử lý vi phạm	Đơn vị quản lý, vận hành hệ thống thông tin phối hợp với các đơn vị liên quan làm rõ nguyên nhân, phân tích ngăn chặn, xử lý kịp thời các đối tượng tấn công, phá hoại, hạn chế đến mức thấp nhất hậu quả xảy ra; nếu nguyên nhân do thiếu trách nhiệm, vi phạm quy định về an toàn thông tin, tùy theo mức độ vi phạm mà tổ chức kiểm điểm rút kinh nghiệm hoặc xử lý theo quy định của pháp luật; nếu nguyên nhân do tác động của các đối tượng tấn công bên ngoài cần thu thập, xác minh, tổng hợp báo cáo chủ quản hệ thống thông tin và cơ quan có thẩm quyền (thuộc Bộ Thông tin và Truyền thông, Cục	Văn phòng Sở, Trung tâm Thông tin và Ứng dụng KHCN	Sở Thông tin và Truyền thông; Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa; Cục Phòng chống tội phạm sử dụng công nghệ cao (Bộ Công an); Cơ quan điều phối quốc gia.

		Phòng chống tội phạm sử dụng công nghệ cao) xem xét, điều tra xử lý.		
IV	**Tổng kết, đánh giá**			
1	Tổng kết, đánh giá	Đơn vị quản lý, vận hành hệ thống thông tin bị sự cố phối hợp với Cơ quan chuyên trách ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh và Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa triển khai tổng hợp toàn bộ các thông tin, báo cáo, phân tích có liên quan đến sự cố, công tác triển khai phương án ứng cứu sự cố, báo cáo Chủ quản hệ thống thông tin, Ban Chỉ đạo chuyển đổi số tỉnh Khánh Hòa và Cơ quan điều phối quốc gia; tổ chức phân tích nguyên nhân, rút kinh nghiệm trong hoạt động xử lý sự cố và đề xuất các biện pháp bổ sung nhằm phòng ngừa, ứng cứu đối với các sự cố tương tự trong tương lai.	Văn phòng Sở, Trung tâm Thông tin và Ứng dụng KHCN	Sở Thông tin và Truyền thông; Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa; Ban Chỉ đạo chuyển đổi số tỉnh Khánh Hòa; Cơ quan điều phối quốc gia.

PHỤ LỤC 2
BẢNG DỰ TOÁN KINH PHÍ

Thực hiện đánh giá các nguy cơ, sự cố an toàn thông tin mạng cho hệ thống thông tin và đào tạo, huấn luyện ứng cứu sự cố an toàn thông tin mạng của Sở Khoa học và Công nghệ năm 2023

(Ban hành kèm theo Kế hoạch số 598 /KH-SKHCN ngày 12 /4/2023 của Sở Khoa học và Công nghệ)

Đơn vị tính: đồng

Số TT	Sản phẩm	Miêu tả sản phẩm	ĐVT	Đơn giá	Thành tiền	Ghi chú
1.	**Dịch vụ**	**Thực hiện đánh giá các nguy cơ, sự cố an toàn thông tin mạng, phòng ngừa, giám sát phát hiện, bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố bao gồm:** - Đánh giá bảo mật vật lý - Đánh giá bảo mật hệ thống mạng - Đánh giá bảo mật hệ thống máy chủ - Đánh giá bảo mật hệ điều hành, dịch vụ - Đánh giá bảo mật cơ sở dữ liệu - Đánh giá bảo mật Portal - Đánh giá bảo mật an toàn Wifi	**Gói**	65.000.000	**65.000.000**	
2.	**Đào tạo, huấn luyện**	**Đào tạo, huấn luyện ứng cứu sự cố ATTT mạng**	**Gói**	42.000.000	**42.000.000**	
				Tổng cộng:	**107.000.000**	