UBND TỈNH KHÁNH HÒA
TRƯỜNG CAO ĐẲNG Y TẾ

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập Tự do – Hạnh phúc

Số: 346/KH- CĐYT

Khánh Hòa, ngày 27 tháng 7 năm 2020

KẾ HOẠCH
Ứng phó sự cố, bảo đảm an toàn thông tin mạng của Trường Cao Đẳng Y tế Khánh Hòa thông năm 2020

Thực hiện Kế hoạch số 860/KH-UBND ngày 30/01/2020 của UBND tỉnh Khánh Hòa về Ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Khánh Hòa năm 2020;

Trường Cao đẳng Y tế Khánh Hòa xây dựng Kế hoạch Ứng phó sự cố, bảo đảm an toàn thông tin mạng năm 2020, cụ thể như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Đảm bảo an toàn thông tin cho các hệ thống thông tin của Trường; 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.

- Tạo chuyển biến mạnh mẽ trong nhận thức về an toàn thông tin đối với cán bộ, giảng viên, nhân viên nhà Trường;

- 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

- Căn cứ trên kết quả khảo sát, đánh giá các nguy cơ, sự cố mất an toàn thông tin mạng của hệ thống thông tin của Trường để đưa ra phương án đối phó, ứng cứu sự cố tương ứng, kịp thời, phù hợp.

- 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 của sự cố khi sự cố xảy ra.

- 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.

II. NHIỆM VỤ TRIỂN KHAI

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

1.1. Tuyên truyền, phổ biến Quyết định số 05/2017/QĐ-TTg và các văn bản quy phạm pháp luật về an toàn thông tin mạng

- **Nội dung thực hiện:** Tổ chức tuyên truyền, phổ biến nội dung của Quyết định số 05/2017/QĐ-TTg; Kế hoạch số 860/KH-UBND và các văn bản quy phạm pháp luật về an toàn thông tin mạng trên Cổng thông tin điện tử của Trường
- **Đơn vị thực hiên:** Phòng Công nghệ thông tin
- **Đơn vị phối hợp:** Các đơn vị, Phòng – Khoa – Bộ môn liên quan
- **Thời gian thực hiện:** Thường xuyên trong năm.

1.2. Tuyên truyền, phổ biến 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 để thực hiện công tác ứng cứu sự cố, bảo đảm an toàn thông tin mạng

- **Nội dung thực hiện**: Tổ chức tuyên truyền, phổ biến, hướng dẫn thực hiện nội dung Thông tư số 121/2018/TT-BTC của Bộ Tài chính trên cổng thông tin điện tử Nhà Trường.
- **Đơn vị thực hiện:** Phòng Công nghệ thông tin
- **Đơn vị phối hợp:** Phòng Kế hoạch - Tài chính
- **Thời gian thực hiện:** Thường xuyên trong năm.

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

- **Nội dung thực hiện:** Tham gia các khóa đào tạo, bồi dưỡng nghiệp vụ phối hợp, ứng cứu, chống tấn công, xử lý mã độc, khắc phục sự cố theo lệnh của cấp trên.
- **Đơn vị thực hiện:** Phòng Công nghệ thông tin.
- **Đơn vị phối hợp:** Các đơn vị, Phòng – Khoa – Bộ môn liên quan
- **Thời gian thực hiện:** Theo kế hoạch, chương trình tập huấn của các cơ quan chuyên môn

1.4. 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; 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:** Phòng Công nghệ thông tin.

- **Đơn vị phối hợp:** Các đơn vị, Phòng – Khoa – Bộ môn liên quan

- **Thời gian thực hiện:** năm 2020

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

- **Nội dung thực hiện:** Nghiên cứu, tham mưu, đề xuất 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:** Phòng Công nghệ thông tin.

- **Đơn vị phối hợp:** Các đơn vị, Phòng – Khoa – Bộ môn liên quan

- **Thời gian thực hiện:** năm 2020

1.6. 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 đối với hệ thống thông tin; đánh giá, dự báo các nguy cơ, sự cố tấn công mạng có thể xảy ra với 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 phục vụ đối phó, ứng cứu, khắc phục sự cố (nếu có).

- **Đơn vị thực hiện:** Phòng Công nghệ thông tin.

- **Đơn vị phối hợp:** Các đơn vị, Phòng – Khoa – Bộ môn liên quan

- **Thời gian thực hiện:** năm 2020

1.7. Xây dựng phương án đối phó, ứng cứu đối với một số tình huống sự cố cụ thể

- **Nội dung thực hiện:** Đối với mỗi hệ thống thông tin và chương trình ứng dụng triển khai tại Trường, cần dự kiến tình huống, sự cố cụ thể và đưa ra phương án đối

phó, ứng cứu sự cố tương ứng. Trong phương án đối phó, ứng cứu phải đặt ra được các tiêu chí để có thể nhanh chóng xác định được tính chất, mức độ nghiêm trọng của sự cố khi sự cố xảy ra. Việc xây dựng phương án đối phó, ứng cứu sự cố cần đảm bảo các nội dung theo hướng dẫn tại Kế hoạch số 860/KH-UBND ngày 30/01/2020 của UBND tỉnh Khánh Hòa

- **Đơn vị thực hiện:** Phòng Công nghệ thông tin.
- **Đơn vị phối hợp:** Các đơn vị, Phòng – Khoa – Bộ môn liên quan
- **Thời gian thực hiện:** năm 2020

2. Triển khai các nhiệm vụ khi có sự cố xảy ra

2.1. Tiếp nhận, phân tích, ứng cứu ban đầu và thông báo sự cố

a. Tiếp nhận, xác minh sự cố

- **Nội dung thực hiện:** Theo dõi, tiếp nhận, phân tích các cảnh báo, dấu hiệu sự cố có thể 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.
- **Đơn vị thực hiện:** Phòng Công nghệ thông tin.
- **Đơn vị phối hợp:** Các đơn vị, Phòng – Khoa – Bộ môn liên quan

b. Triển khai các bước ưu tiên ứng cứu ban đầu

- **Nội dung thực hiện:** Sau khi đã xác định sự cố xảy ra, đơn vị sử dụng, vận hành hệ thống thông tin cần căn cứ vào dấu hiệu, cảnh báo, hướng dẫn của cơ quan chuyên môn để tổ chức triển khai các bước ưu tiên ban đầu để xử lý sự cố.
- **Đơn vị thực hiện:** Phòng Công nghệ thông tin.
- **Đơn vị phối hợp:** Các đơn vị, Phòng – Khoa – Bộ môn liên quan

c. Triển khai lựa chọn phương án ứng cứu

- **Nội dung thực hiện:** Căn cứ theo các cảnh báo, hướng dẫn của cơ quan chuyên trách ứng cứu sự cố an toàn thông tin mạng để lựa chọn phương án ngăn chặn và xử lý sự cố. Báo cáo, đề xuất Ban giám hiệu xin ý kiến chỉ đạo.
- **Đơn vị thực hiện:** Phòng Công nghệ thông tin.
- **Đơn vị phối hợp:** Các đơn vị, Phòng – Khoa – Bộ môn liên quan

2.2. Triển khai ứng cứu, ngăn chặn và xử lý sự cố

- **Nội dung thực hiện:** 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.

- **Đơn vị thực hiện:** Phòng Công nghệ thông tin.

- **Đơn vị phối hợp:** Các đơn vị, Phòng – Khoa – Bộ môn liên quan

2.3. Xử lý sự cố, gỡ bỏ và khôi phục

a. Xử lý sự cố, gỡ bỏ

- **Nội dung thực hiện:** Sau khi đã triển khai ngăn chặn sự cố, Đơn vị quản lý, vận hành hệ thống thông tin khẩn trương 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.

- **Đơn vị thực hiện:** Phòng Công nghệ thông tin.

- **Đơn vị phối hợp:** Các đơn vị, Phòng – Khoa – Bộ môn liên quan

b. Khôi phục

- **Nội dung thực hiện**: 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.

- **Đơn vị thực hiện:** Phòng Công nghệ thông tin.

- **Đơn vị phối hợp:** Các đơn vị, Phòng – Khoa – Bộ môn liên quan

c. Kiểm tra, đánh giá hệ thống thông tin

- **Nội dung thực hiện:** Đơn vị sử dụng, quản lý, vận hành hệ thống thông tin và các cơ quan, 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.

- **Đơn vị thực hiện:** Phòng Công nghệ thông tin.

- **Đơn vị phối hợp:** Các đơn vị, Phòng – Khoa – Bộ môn liên quan

III. KINH PHÍ THỰC HIỆN

Căn cứ tình hình thực tế, Phòng Công nghệ thông tin phối hợp Phòng Kế hoạch – Tài chính tham mưu Ban giám hiệu đề xuất kinh phí trong quá trình triển khai phương án ứng cứu sự cố.

IV. TỔ CHỨC THỰC HIỆN

- Phổ biến Kế hoạch ứng phó sự cố, bảo đảm an toàn thông tin mạng của nhà trường trên cổng thông tin điện tử, bảo đảm đúng tiến độ, chất lượng, hiệu quả, tránh hình thức.

- Thực hiện bố trí cán bộ, đảm bảo an toàn thông tin Nhà trường; kịp thời thông báo về Sở Thông tin và Truyền thông khi có sự thay đôi cán bộ tham mưu công tác đảm báo an toàn thông tin mạng cùa trường.

- Phòng Công nghệ thông tin là đơn vị đầu mối về ứng cứu sự cố an toàn thông tin mạng của Nhà trường.

- Phòng Kế hoạch -Tài chính phối hợp với phòng Công nghệ thông tin, các đơn vị liên quan thẩm định và tham mưu Ban giám hiệu bố trí kinh phí để thực hiện các nội dung theo Kế hoạch.

KT HIỆU TRƯỞNG

PHÓ HIỆU TRƯỞNG

Nơi nhận:
- Sở TTTT;
- Lưu : VT, P.CNTT;

ỦY BAN NHÂN DÂN TỈNH KHÁNH HÒA
TRƯỜNG CAO ĐẲNG Y TẾ KHÁNH HÒA

Đỗ Anh Thư