SỞ GDĐT TỈNH BÌNH DƯƠNG
TRƯỜNG THPT NGUYỄN ĐÌNH CHIỂU

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

Số: 548/PA-THPTNĐC

Thủ Dầu Một, ngày 31 tháng 08 năm 2024

PHƯƠNG ÁN
Tăng cường công tác bảo đảm an toàn thông tin mạng trong thời gian nghỉ lễ Quốc khánh 02/9

Căn cứ Công văn số 2280/SGDĐT-VP ngày 30/8/2024 của Sở GDĐT tỉnh Bình Dương về việc tăng cường công tác bảo đảm an toàn thông tin mạng trong thời gian nghỉ lễ Quốc khánh 02/9.

Trường THPT Nguyễn Đình Chiểu xây dựng kế hoạch tăng cường công tác bảo đảm an toàn thông tin mạng trong thời gian nghỉ lễ Quốc khánh 02/9, 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. NỘI DUNG THỰC HIỆN

1. Triển khai các nhiệm vụ sẵn sàng bảo đảm an toàn thông tin

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

Tổ chức tuyên truyền, phổ biến, nâng cao nhận thức, trách nhiệm và các kỹ năng cơ bản bảo đảm an toàn thông tin trên không gian mạng qua các phương tiện thông tin đại chúng, truyền thông xã hội.

1.2. Tham gia huấn luyện, diễn tập phòng ngừa sự cố, giám sát phát hiện, bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố

Tham gia tập huấn, bồi dưỡng ngắn hạn về an toàn thông tin do các cấp, các ngành tổ chức.

1.3. Triển khai phòng ngừa sự cố, giám sát phát hiện sớm sự cố

Tập trung triển khai các biện pháp bảo vệ an toàn thông tin cho các hệ thống thông tin; sắp xếp, bố trí cán bộ đủ năng lực chuyên môn, có phẩm chất tốt để đảm nhiệm những vị trí quan trọng trong quản lý, vận hành các hệ thống thông tin. Chú trọng vấn đề nâng cấp bảo mật cho các hệ thống thông tin, cơ sở hạ tầng mạng trong hệ thống thông tin của cơ quan.

Thực hiện các đợt tấn công mô phỏng thực tế có kiểm soát (pentest) nhằm đánh giá mức độ an toàn của các hệ thống thông tin nhằm phát hiện kịp thời những điểm yếu tiềm tàng của các hệ thống thông tin. Từ đó báo cáo và đưa ra các giải pháp bảo mật phù hợp và nâng cấp để hạn chế các nguy cơ đối với hệ thống thông tin

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

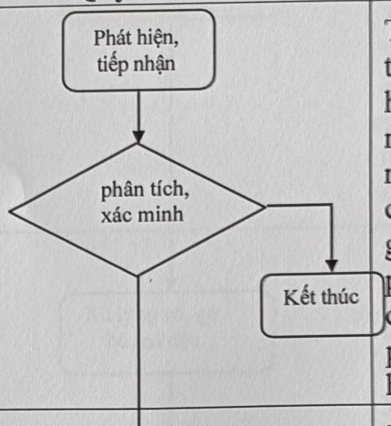
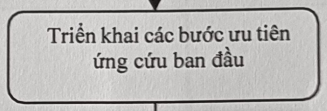
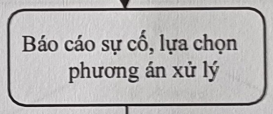
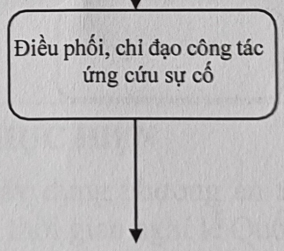
Trang bị, nâng cấp trang thiết bị, công cụ, phương tiện, bản quyền của các phần mềm phục vụ ứng cứu, khắc phục sự cố; chuẩn bị các điều kiện bảo đảm, dự phòng các nguồn lực và tài chính để sẵn sàng đối phó, ứng cứu, khắc phục khi sự cố xảy ra; tổ chức hoạt động của Đội ứng cứu sự cố; tổ chức và tham gia các hoạt động của mạng lưới ứng cứu sự cố.

1.5. Kiểm tra, đánh giá các nguy cơ, sự cố an toàn thông tin mạng

Tổ chức kiểm tra, 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 hệ thống thông tin có thể xảy ra; dự báo đối tượng có thể tấn công, phá hoại gây ra sự cố mất an toàn thông tin mạng; 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 của đơn vị (bao gồm của cả đơn vị đã ký hợp đồng cung cấp dịch vụ).

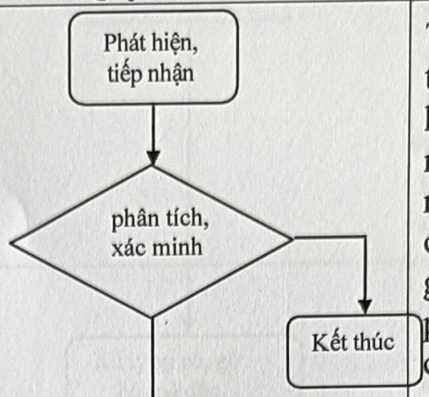
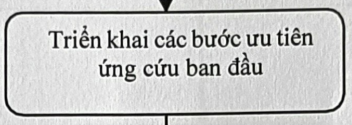
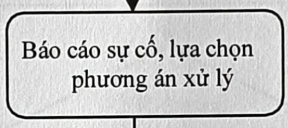
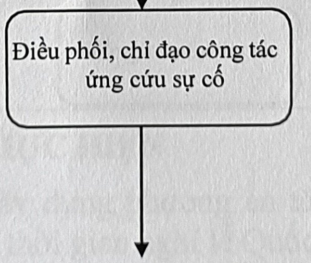
2. Triển khai các nhiệm vụ khi có sự cố xảy ra

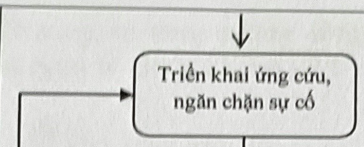
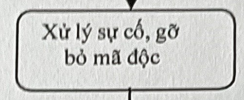
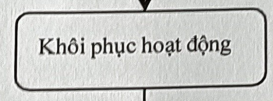
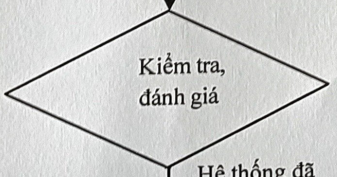
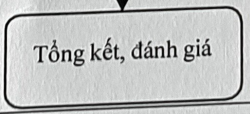
Thực hiện theo Quy trình ứng cứu, xử lý khẩn cấp sự cố tấn công mạng:

Thành phần	Quy trình	Ghi chú
Đơn vị quản lý, vận hành hệ thống thông tin		Theo dõi, tiếp nhận, phân tích các cảnh báo, dấu hiệu sự cố có thể từ các nguồn bên trong và bên ngoài; ghi nhận, thu thập chứng cứ, xác định nguồn gốc sự cố nhằm áp dụng phương án đối phó, ứng cứu, khắc phục sự cố phù hợp
Đơn vị quản lý, vận hành hệ thống thông tin		Triển khai các bước ưu tiên ban đầu để xử lý sự cố theo phương án, kế hoạch ứng phó sự cố; kịp thời phân tích và xác định tình hình sự cố để xác định phạm vi ảnh hưởng
Đơn vị quản lý, vận hành hệ thống thông tin		Thông báo, báo cáo sự cố đến các tổ chức, cá nhân liên quan bên trong và bên ngoài cơ quan theo quy định; tiến hành lựa chọn phương án ngăn chặn và xử lý sự cố.
Ban chỉ đạo Chuyển đổi số		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.

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:

Thành phần	Quy trình	Ghi chú
Đơn vị quản lý, vận hành hệ thống thông tin		Theo dõi, tiếp nhận, phân tích các cảnh báo, dấu hiệu sự cố có thể từ các nguồn bên trong và bên ngoài; ghi nhận, thu thập chứng cứ, xác định nguồn gốc sự cố nhằm áp dụng phương án đối phó, ứng cứu, khắc phục sự cố phù hợp
Đơn vị quản lý, vận hành hệ thống thông tin		Triển khai các bước ưu tiên ban đầu để xử lý sự cố theo phương án, kế hoạch ứng phó sự cố; kịp thời phân tích và xác định tình hình sự cố để xác định phạm vi ảnh hưởng
Đơn vị quản lý, vận hành hệ thống thông tin		Thông báo, báo cáo sự cố đến các tổ chức, cá nhân liên quan bên trong và bên ngoài cơ quan theo quy định; tiến hành lựa chọn phương án ngăn chặn và xử lý sự cố.
Ban chỉ đạo Chuyển đổi số		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.

Đơn vị quản lý, vận hành hệ thống thông tin; Đội ứng cứu 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.
Đơn vị quản lý, vận hành hệ thống thông tin; Đội ứng cứu sự cố		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.
Đơn vị quản lý, vận hành hệ thống thông tin.	 Hệ thống chưa hoạt	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 quản lý, vận hành hệ thống thông tin.	động bình thường  Hệ thống đã hoạt động bình	Kiểm tra, đánh giá hoạt động của toàn bộ hệ thống thông tin sau khi khắc phục sự cố
Đơn vị quản lý, vận hành hệ thống thông tin.		Tổng hợp, báo cáo, phân tích nguyên nhân, rút kinh nghiệm.

III. TỔ CHỨC THỰC HIỆN

- Ban Giám hiệu xây dựng phương án tăng cường công tác bảo đảm an toàn thông tin mạng trong thời gian nghỉ lễ Quốc khánh 02/9.

- Bộ phận CNTT có trách nhiệm tham mưu và triển khai thực hiện phương án đạt hiệu quả; đồng thời tổng hợp báo cáo Ban Giám hiệu kết quả thực hiện tăng cường công tác bảo đảm an toàn thông tin mạng trong thời gian nghỉ lễ Quốc khánh 02/9.

Trên đây là Phương án tăng cường công tác bảo đảm an toàn thông tin mạng trong thời gian nghỉ lễ Quốc khánh 02/9 của Trường THPT Nguyễn Đình Chiểu./.

Nơi nhận:
- Ban giám hiệu;
- Chủ tịch Công đoàn;
- Bí thư Đoàn thanh niên;
- Tổ trưởng chuyên môn;
- Tổ trưởng Văn phòng;
- Giáo viên chủ nhiệm 29 lớp;
- Vnedu; Bảng tin;
- Lưu: VT, B.

HIỆU TRƯỞNG

SỞ GIÁO DỤC VÀ ĐÀO TẠO TỈNH BÌNH DƯƠNG
TRƯỜNG TRUNG HỌC PHỔ THÔNG NGUYỄN ĐÌNH CHIỂU

Phạm Nguyễn Thanh Tuấn