UBND HUYỆN TÂN HỒNG
TRƯỜNG THCS NGUYỄN DU

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

Số: 12 /KH THCSND

Tân Hồng, ngày 05 tháng 01 năm 2022

KẾ HOẠCH
Ứng phó sự cố, bảo đảm an toàn thông tin mạng trong nhà trường giai đoạn 2021 - 2025

Căn cứ kế hoạch số 301/KH-UBND ngày 28 tháng 12 năm 2021 của Ủy ban nhân dân huyện Tân Hồng về việc ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn huyện Tân Hồng giai đoạn 2021 – 2025;

Căn cứ kế hoạch số 1654/KH-PGDĐT ngày 31 tháng 12 năm 2021 của Phòng giáo dục huyện Tân Hồng về việc ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn huyện Tân Hồng giai đoạn 2021 – 2025;

Nay trường THCS Nguyễn Du xây dựng Kế hoạch ứng phó sự cố, bảo đảm an toàn thông tin mạng trong nhà trường giai đoạn 2021 - 2025 như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Bảo đảm an toàn thông tin cho các hệ thống thông tin quan trọng trong ngành giáo dục và đào tao; khả năng thích ứng một cách chủ động, linh hoạt, giảm thiểu các nguy cơ mất an toàn thông tin trên mạng; đề ra các phương án ứng phó khi phát sinh sự cố mất an toàn thông tin mạng.

- Bảo đảm các điều kiện cần thiết để triển khai kịp thời các phương án ứng cứu khẩn cấp sự cố an toàn thông tin mạng.

- Nâng cao nhận thức, kỹ năng về bảo đảm an toàn thông tin mạng cho cán bộ, công chức, viên chức và người lao động.

2. Yêu cầu

- Căn cứ kết quả giám sát, khảo sát và đánh giá nguy cơ mất an toàn thông tin mạng của các hệ thống thông tin trong nhà trường để đưa ra các phương án ứng phó phù hợp.

- Xây dựng kế hoạch đề ra các tiêu chí để kịp thời xác định tính chất, mức độ nghiêm trọng của sự cố khi có sự cố xảy ra.

- Triển khai các nội dung của Kế hoạch, bảo đảm khả thi, hiệu quả.

II. NHIỆM VỤ TRIỂN KHAI

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

- Tuyên truyền, phổ biến Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 và các văn bản quy phạm pháp luật về an toàn thông tin mạng và Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 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.

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

a) Tiếp nhận, phân tích, ứng cứu ban đầu và thông báo sự cố

- Tiếp nhận, xác minh sự cố: Theo dõi, tiếp nhận, phân tích các cảnh báo, dấu hiệu sự cố 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

- Sau khi đã xác định sự cố xảy ra, 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 theo hướng dẫn của Đơn vị chuyên trách về ứng cứu sự cố liên quan.

- Báo cáo sự cố.

b) 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.

- Triển khai 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.

c) Xử lý sự cố, gỡ bỏ mã độc và khôi phục hệ thống

- Xử lý sự cố, gỡ bỏ mã độc: Sau khi đã triển khai ngăn chặn sự cố, Nhà trường vận hành hệ thống thông tin triển khai 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.

- Khôi phục hệ thống: 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 cho hệ thống thông tin.

- Kiểm tra, đánh giá hệ thống thông tin: Kiểm tra, đánh giá hoạt động của toàn bộ hệ thống thông tin sau khi khắc phục sự cố.

III. TỔ CHỨC THỰC HIỆN

- Căn cứ nội dung Kế hoạch này, tình hình thực tế các bộ phận có liện quan trong nhà trường triển khai dầu mối là Giáo viên phụ trách công nghệ thông tin tham mưu thực hiện phương án đối phó, ứng cứu sự cố an toàn thông tin mạng tại đơn vị theo đề cương phụ lục của quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ.

- Nhà trường Giao cho giáo viên phụ trách công nghệ thông tin bảo đảm an toàn thông tin mạng tại trường và báo cáo về Phòng Giáo dục và Đào tạo để tổng hợp thông tin kịp thời qua Phòng Văn hoá và Thông tin.

- Định kỳ ngày 10/6 báo cáo 6 tháng, báo cáo năm trước ngày 10/12 kết quả thực hiện về Phòng Giáo dục và Đào tạo (qua phần mềm iDesk).

Trên đây là Kế hoạch ứng phó sự cố, bảo đảm an toàn thông tin mạng trong nhà trường giai đoạn 2021 – 2025 của trường THCS Nguyễn Du./.

Nơi nhận:
-Phòng GD (báo cáo);
- BGH- GVNV (thực hiện);
-Lưu:VT.

HIỆU TRƯỞNG

Nguyễn Văn Đồng Tiến

Phụ lục II

TRIỂN KHAI CÁC NHIỆM VỤ KHI CÓ SỰ CỐ XẢY RA

(kèm theo Kế hoạch số: /KH THCSND ngày tháng 01 năm 2022 của Tường THCS Nguy)

Stt	Nhiệm vụ
1	Theo dõi, tiếp nhận, phân tích các cảnh báo, dấu hiệu sự cố có thể từ các nguồn bên trong và bên ngoài *(tổ chức ghi nhận, thu thập chứng cứ, xác định nguồn gốc sự cố)*
2	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 đối với nhà trường
3	Lựa chọn phương án ngăn chặn và xử lý sự cố; báo cáo, đề xuất chủ quản hệ thống thông tin
5	Báo cáo sự cố đến các tổ chức, cá nhân liên quan bên trong và bên ngoài nhà trường, tổ chức theo quy định tại Điều 9 Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 và quy định nội bộ *(nếu có)*
6	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.
7	Gỡ bỏ các mã độc, phần mềm độc hại, khắc phục các điểm yếu an toàn thông tin của hệ thống thông tin.
8	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 cho hệ thống thông tin.
9	Kiểm tra, đánh giá hoạt động của toàn bộ hệ thống thông tin sau khi khắc phục sự cố. Trường hợp hệ thống chưa hoạt động ổn định, cần tiếp tục tổ chức thu thập, xác minh lại nguyên nhân, xử lý dứt điểm, khôi phục hoạt động bình thường của hệ thống thông tin.
10	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; đồng thời, 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.