

Số: /KH-SGDĐT

Tây Ninh, ngày 01 tháng 02 năm 2021

KẾ HOẠCH

đảm bảo an toàn an ninh thông tin, hệ thống thông tin của Ngành Giáo dục và Đào tạo

Thực hiện Kế hoạch số 231/KH-UBND ngày 25/01/2020 của UBND tỉnh về việc đảm bảo an toàn an ninh thông tin các hệ thống thông tin của tỉnh trong thời gian Đại hội lần thứ XIII của Đảng và các dịp lễ, tết trong năm 2021, để tăng cường bảo đảm an toàn, an ninh mạng, không để bị động, bất ngờ với mọi tình huống tấn công mạng và phát tán thông tin xấu độc trong Ngành Giáo dục, Sở Giáo dục và Đào tạo ban hành kế hoạch đảm bảo an toàn an ninh thông tin, hệ thống thông tin của Sở, cụ thể như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Quy định trình tự, cách thức thực hiện, kiểm soát việc xử lý sự cố khi bị tấn công mạng hoặc xảy ra sự cố đối với hệ thống thông tin gây ảnh hưởng đến hoạt động của Sở Giáo dục và Đào tạo.
- Đảm bảo hoạt động ổn định xuyên suốt trang thông tin Sở (www.tayninh.edu.vn) và hệ thống phần mềm dùng chung của tỉnh, các hệ thống phần mềm của các Sở đang vận hành.

2. Yêu cầu

- Phòng Khảo thí – CNTT khắc phục sự cố và phục hồi hoạt động của hệ thống thông tin một cách nhanh nhất. Duy trì hoạt động bình thường của hệ thống thông tin, không để Hệ thống thông tin Sở bị phá hoại, lộ lọt thông tin.
- Phòng Khảo thí – CNTT phối hợp tham mưu Ban Giám đốc đảm bảo cơ sở vật chất, nguồn lực phải được ưu tiên cho công tác xử lý sự cố.
- Phòng Khảo thí – CNTT báo cáo ngay cho Ban Giám đốc khi xảy ra sự cố gây mất an toàn thông tin trong Ngành Giáo dục.

II. NỘI DUNG

1. Tuyên truyền, phổ biến các văn bản quy phạm pháp luật để nâng cao nhận thức, kiến thức, kỹ năng về an toàn thông tin mạng

- Sở Giáo dục và Đào tạo tổ chức tuyên truyền, phổ biến về Luật An toàn thông tin mạng; Luật An ninh mạng; 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; 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; Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị

định 85/2016/NĐ-CP ; 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 để nâng cao nhận thức, kiến thức, kỹ năng về an toàn thông tin mạng cho cán bộ, công chức, viên chức trên công thông tin điện tử.

2. Rà soát các nguy cơ, sự cố an toàn thông tin mạng của Ngành

Sở Giáo dục và Đào tạo phối hợp với Sở Thông tin và Truyền thông: thường xuyên kiểm tra hiện trạng và khả năng bảo đảm an toàn thông tin mạng của Ngành và hệ thống cơ sở dữ liệu cần bảo vệ, dự báo các nguy cơ, sự cố, tấn công mạng có thể xảy ra, dự báo các hậu quả, thiệt hại, tác động có thể có nếu xảy ra sự cố; chú ý xem xét hiện trạng phương tiện, trang thiết bị, nhân lực, vật lực phục vụ đối phó, ứng cứu, khắc phục sự cố.

3. Xây dựng phương án đối phó, ứng cứu

3.1. Phương pháp, cách thức để xác định kịp thời nguyên nhân, nguồn gốc sự cố nhằm áp dụng phương án đối phó, ứng cứu, khắc phục sự cố phù hợp:

- Sự cố do bị tấn công mạng;
- Sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật hoặc do lỗi đường điện, đường truyền, hosting...;
- Sự cố do lỗi của người quản trị, vận hành hệ thống;
- Sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn v.v...

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

- Tình huống sự cố do bị tấn công mạng:
 - + Tấn công từ chối dịch vụ;
 - + Tấn công giả mạo;
 - + Tấn công sử dụng mã độc;
 - + Tấn công truy cập trái phép, chiếm quyền điều khiển;
 - + Tấn công thay đổi giao diện;
 - + Tấn công mã hóa phần mềm, dữ liệu, thiết bị;
 - + Tấn công phá hoại thông tin, dữ liệu, phần mềm;
 - + Tấn công nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu;
 - + Tấn công tổng hợp sử dụng kết hợp nhiều hình thức;
 - + Các hình thức tấn công mạng khác.
- Tình huống sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật:
 - + Sự cố nguồn điện;
 - + Sự cố đường kết nối Internet;
 - + Sự cố do lỗi phần mềm, phần cứng, ứng dụng của hệ thống thông tin;
 - + Sự cố liên quan đến quá tải hệ thống;

- + Sự cố khác do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật.
- Tình huống sự cố do lỗi của người quản trị, vận hành hệ thống:
- + Lỗi trong cập nhật, thay đổi, cấu hình phần cứng;
- + Lỗi trong cập nhật, thay đổi, cấu hình phần mềm;
- + Lỗi liên quan đến chính sách và thủ tục an toàn thông tin;
- + Lỗi liên quan đến việc dừng dịch vụ vì lý do bắt buộc;
- + Lỗi khác liên quan đến người quản trị, vận hành hệ thống.
- Tình huống sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn v.v....

3.3. Phối hợp với Sở Thông tin và Truyền thông, VNPT Tây Ninh, Viettel Tây Ninh trong đối phó, ngăn chặn, ứng cứu, khắc phục sự cố.

3.4. Phòng Khảo thí – Công nghệ thông tin: xem xét tham mưu nhân lực, trang thiết bị, phần **mềm**, phương tiện, công cụ và dự kiến kinh phí để thực hiện, đối phó, ứng cứu, xử lý đối với từng tình huống sự cố cụ thể.

4. Triển khai hoạt động điều phối, xử lý, ứng cứu sự cố

Triển khai trách nhiệm của Ngành theo quy định tại Điều 11, Điều 12, Điều 13, Điều 14 của 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.

Báo cáo về Sở Thông tin và Truyền thông các sự cố an toàn thông tin mạng theo quy định tại Điều 11 Quyết định số 05/2017/QĐ-TTg, Điều 9 Thông tư 20/2017/TT-BTTTT.

Dự trù kinh phí, nhân lực, vật lực sẵn sàng ứng cứu sự cố và thực hiện ứng cứu, xử lý, ngăn chặn, khắc phục sự cố khi có sự cố xảy ra.

5. Triển khai phòng ngừa sự cố, bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố

Sở Giáo dục và Đào tạo xây dựng các nội dung, nhiệm vụ cụ thể cần triển khai nhằm phòng ngừa sự cố, giám sát phát hiện, bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố, triển khai các phương án đối phó, ứng cứu sự cố tương ứng với các kịch bản, tình huống sự cố cụ thể; chỉ đạo nâng cao kỹ năng, nghiệp vụ phối hợp, ứng cứu, chống tấn công, xử lý mã độc, khắc phục sự cố, vận hành hệ thống thông tin đúng theo quy chế an toàn thông tin.

Sở Giáo dục và Đào tạo chú trọng nội dung, nhiệm vụ nhằm phòng ngừa sự cố và phát hiện sớm sự cố: kiểm tra, chú ý 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.

Sở Giáo dục và Đào tạo chú trọng trang bị, nâng cấp trang thiết bị, công cụ, phương tiện, 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; thuê dịch vụ kỹ thuật; tổ chức và tham gia các hoạt động của mạng lưới ứng cứu sự cố do Sở Thông tin và Truyền thông tổ chức.

III. TỔ CHỨC THỰC HIỆN

- Phòng Khảo thí - CNTT chịu trách nhiệm về an toàn thông tin mạng của Sở.

- Phòng Khảo thí – CNTT: Xây dựng nội dung để triển khai các nhiệm vụ được giao tại Kế hoạch này.

- Phòng Khảo thí – CNTT: Thông báo, phối hợp với các đơn vị có liên quan khi xảy ra sự cố gây mất an toàn thông tin.

- Phối hợp với Sở Thông tin và Truyền thông: có kế hoạch đảm bảo an toàn thông tin cho Ngành, tiếp nhận và xử lý các sự cố về ATTT mạng, tham mưu, kiểm tra, đánh giá, giám sát công tác bảo đảm an toàn thông tin của Ngành hàng năm.

- Phối hợp với Công an tỉnh: ứng phó sự cố an toàn thông tin, chú ý công tác phòng, chống, điều tra tội phạm lợi dụng hệ thống mạng để xâm phạm an ninh, gây mất an toàn thông tin mạng, mất trật tự trong toàn Ngành.

- Hỗ trợ các đơn vị, trường học đánh giá nguy cơ mất an toàn thông tin mạng khi có yêu cầu.

Trên đây là Kế hoạch ứng phó sự cố đảm bảo an toàn thông tin mạng của Sở Giáo dục và Đào tạo yêu cầu Thủ trưởng các đơn vị, trường học nghiêm túc triển khai thực hiện. Trong quá trình thực hiện nếu có khó khăn, vướng mắc đề nghị các đơn vị, trường học phản ánh về Phòng Khảo thí – Công nghệ thông tin để tổng hợp báo cáo Ban Giám đốc chỉ đạo giải quyết kịp thời./.

Nơi nhận:

- Sở TTTT (báo cáo);
- Các đơn vị, trường học (thực hiện);
- Ban Giám đốc;
- Các phòng chuyên môn (phối hợp);
- Lưu: VT, KT.

GIÁM ĐỐC