UBND HUYỆN MƯỜNG CHÀ
TRƯỜNG PTDTBT TH MƯỜNG ANH

Số: 45/KH-PTDTBT-THMA

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

Pa Ham, ngày 20 tháng 12 năm 2024

KẾ HOẠCH
Ứng phó sự cố và đảm bảo an toàn thông tin

Thực hiện Kế hoạch số 3055/KH-SGDĐT ngày 04 tháng 11 năm 2024 của Sở Giáo dục và Đào tạo tỉnh Điện Biên về kế hoạch ứng phó sự cố và đảm bảo an toàn thông tin Nghành Giáo dục.

Trường PTDTBT tiểu học Mường Anh xây dựng kế hoạch ứng phó sự cố và đảm bảo an toàn thông tin như sau:

I. MỤC ĐÍCH YÊN CẦU

1. Mục đích

Đảm bảo an toàn, an ninh thông tin mạng phục vụ công tác quản lý, công tác dạy - học và các hoạt động khác trong nhà trường trên các hệ thống thông tin ngành giáo dục và đào tạo, tăng khả năng thích ứng linh hoạt, giảm thiểu các nguy cơ, đe dọa mất an toàn thông tin mạng và chủ động phòng ngừa, ứng phó khi có sự cố về an toàn thông tin.

Triển khai các nhiệm vụ ứng phó sự cố và đảm bảo an toàn thông tin mạng theo hướng dẫn của Sở GD&ĐT, Phòng GD&ĐT.

2. Yêu cầu

100% hệ thống thông tin của của nhà trường được phê duyệt cấp độ an toàn hệ thống thông tin và triển khai các đầy đủ phương án đảm bảo an toàn thông tin theo Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ và Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông.

Các máy tính phục vụ công tác hành chính của nhà trường phải cài đặt phần mềm phòng, chống mã độc và chia sẻ thông tin với Trung tâm Giám sát an toàn không gian mạng quốc gia.

Ban hành các quy định, quy chế và hướng dẫn về đảm bảo an toàn, an ninh thông tin trong hoạt động của đơn vị.

Thành lập tổ an toàn thông tin và phân công cán bộ kiêm nhiệm an toàn thông tin của đơn vị, có khả năng phòng thủ, ứng phó với các nguy cơ và sự cố mất an toàn thông tin trên không gian mạng đối với các hệ thống thông tin.

Các hệ thống thông tin của nhà trường được đầu tư hoàn thiện, nâng cao khả năng phòng, chống các cuộc tấn công trên môi trường mạng.

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.

Phối hợp chặt chẽ với Đội Ứng cứu sự cố an toàn thông tin mạng của Sở Giáo dục, Phòng Giáo dục trong quá trình triển khai thực hiện. Đảm bảo các nguồn lực và các điều kiện cần thiết để sẵn sàng triển khai kịp thời, hiệu quả phương án ứng cứu sự cố bảo đảm an toàn thông tin mạng trong hoạt động của đơn vị.

II. NỘI DUNG THỰC HIỆN

1. Đánh giá nguy cơ, sự cố an toàn thông tin mạng

Các hệ thống thông tin yêu cầu phải đánh giá gồm: Các hệ thống thông tin, ứng dụng công nghệ thông tin của Trường PTDTBT tiểu học Mường Anh; các hệ thống thông tin được vận hành, hệ thống mạng máy tính nội bộ (LAN) của Trường PTDTBT tiểu học Mường Anh.

2. Đầu tư trang thiết bị, phần mềm thiết yếu bảo đảm an toàn thông tin

Đầu tư, quản lý, khai thác các trang thiết bị thiết yếu bảo đảm an toàn thông tin cho cơ quan, đơn vị gồm: Thiết bị tường lửa mạng (Network fire wall), thiết bị phục vụ quản trị, giám sát an ninh mạng...

Sử dụng phần mềm virus có bản quyền quản lý tập trung áp ứng yêu cầu bảo vệ máy tính và giám sát an ninh cho 100% máy tính trong mạng của cơ quan, đơn vị theo hướng ưu tiên sử dụng các giải pháp phần mềm virus có bản quyền quản lý tập trung (Endpoint security).

3. Triển khai các hoạt động thường trực, điều phối, xử lý, ứng cứu sự cố

3.1. Tiếp nhận, xác định sự cố:

Thành viên Tổ Ứng dụng Công nghệ thông tin, Chuyển đổi số. Trường PTDTBT tiểu học Mường Anh trao đổi, liên hệ Đội Ứng cứu sự cố an toàn thông tin mạng của tỉnh tiếp nhận, phân tích các cảnh báo, dấu hiệu sự cố từ các nguồn bên trong và bên ngoài (cảnh báo sự cố: Văn bản, email, điện thoại, website, facebook, mạng xã hội...; phát hiện sự cố thông qua kiểm tra, rà soát, đánh giá). Khi xác định được sự cố đã xảy ra, cần tổ chức 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:

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;

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...

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

Sau khi đã xác định sự cố xảy ra, thành viên Tổ UDCNTT của Trường PTDTBT tiểu học Mường Anh riển khai các bước ưu tiên ban đầu để xử lý sự cố theo phương án, kế hoạch ứng phó sự cố đã được cấp thẩm quyền phê duyệt/xác nhận hoặc theo tư vấn, hướng dẫn của Đội Ứng cứu sự cố an toàn thông tin mạng của huyện.

Tổ UDCNTT phải kịp thời phân tích và xác định tình hình sự cố để xác định phạm vi ảnh hưởng. Những phân tích ban đầu sẽ cung cấp thông tin cho các hoạt động tiếp theo.

3.3. Ngăn chặn, xử lý sự cố

Trường PTDTBT tiểu học Mường Anh vận hành hệ thống phối hợp với thành viên Tổ UDCNTT và các đơn vị liên quan báo cáo, đề xuất cơ quan chủ quản hệ thống thông tin, Tổ UDCNTT phê duyệt phương án, chiến lược ngăn chặn và xử lý sự cố và đề nghị hỗ trợ từ cơ quan nếu cần thiết.

3.4. Xác định nguồn gốc tấn công

Thành viên Tổ UDCNTT triển khai phân tích, xác định nguồn gốc tấn công để ngăn chặn, giảm thiểu tác động, thiệt hại đến hệ thống thông tin.

3.5. Khắc phục, gỡ bỏ sự cố

Sau khi đã triển khai ngăn chặn sự cố, phải tiến hành tiêu diệt các mã độc, phần mềm độc hại, khắc phục các điểm yếu ATTT của hệ thống (xây dựng lại hệ thống, thay thế các tệp tin bị lỗi, cài đặt các bản vá lỗi, thay đổi mật khẩu và rà soát các chính sách ATTT).

3.6. Khôi phục

Triển khai các hoạt động khôi phục hệ thống, dữ liệu và kết nối (phải khôi phục từ các bản sao lưu hệ thống "sạch"); cấu hình hệ thống an toàn; bổ sung các thiết bị, phần cứng, phần mềm bảo đảm ATTT cho hệ thống thông tin và kiểm tra thử toàn bộ hệ thống sau khi khắc phục sự cố.

IV. TỔ CHỨC THỰC HIỆN

1. Lãnh đạo nhà trường

Hiệu trưởng trường PTDTBT tiểu học Mường Anh chỉ đạo tổ chức, triển khai thực hiện Kế hoạch trong đơn vị; thường xuyên phối hợp với thành viên tổ ƯDCNTT; Đội ứng cứu sự cố an toàn thông tin trường thực hiện các nhiệm vụ ứng phó sự cố và đảm bảo an toàn thông tin mạng.

Triển khai đầy đủ các quy định về đảm bảo an toàn thông tin theo cấp độ đối với hệ thống thông tin do đơn vị chủ trì xây dựng hoặc thuê dịch vụ công nghệ thông tin theo Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ và Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông.

Tăng cường công tác tuyên truyền nâng cao nhận thức về an toàn, an ninh thông tin mạng cho viên chức và người lao động đơn vị.

Chủ động bố trí kinh phí và tăng cường thực hiện các biện pháp đảm bảo an toàn, an ninh thông tin đối với các hệ thống máy tính, hệ thống thông tin đang triển khai, ứng dụng tại đơn vị.

Tăng cường kiểm tra, đánh giá định kỳ về an toàn thông tin mạng đối với các hệ thống thông tin của đơn vị; đầu tư thiết bị để nâng cao năng lực phòng, chống tấn công mạng đối với các hệ thống thông tin.

Tập huấn về an toàn thông tin, nâng cao kỹ năng an toàn thông tin cho đội ngũ viên chức, người lao động nhà trường trên môi trường mạng. Cử cán bộ phụ trách về an toàn thông tin/chuyển đổi số tham gia các khóa đào tạo, tập huấn về an toàn thông tin.

Kịp thời cung cấp thông tin, số liệu về pháp lý, kỹ thuật, tổ chức, nâng cao năng lực và hợp tác trong lĩnh vực an toàn, an ninh mạng phục vụ việc đánh giá xếp hạng chỉ số An toàn thông tin.

Phân công cán bộ, viên chức kiêm nhiệm làm công tác chuyển đổi số, công tác an toàn thông tin mạng tại cơ quan, đơn vị.

2. Bộ phận chuyên môn

Căn cứ nội dung chương trình, xây dựng kế hoạch lồng ghép các hoạt động về an toàn thông tin mạng vào các hoạt động giáo dục phù hợp với điều kiện của nhà trường để đạt hiệu quả cao.

3. Ban chấp hành công đoàn trường

Phối hợp đẩy mạnh công tác truyền thông, nâng cao nhận thức, kỹ năng số, kỹ năng khai thác thông tin an toàn trên môi trường mạng trong lực lượng đoàn viên công đoàn nhà trường.

Vận động đoàn viên và người lao động nâng cao trách nhiệm bản thân trong việc thực hiện tốt văn hóa giao tiếp và khai thác thông tin trên không gian mạng.

Kịp thời báo cáo những sự cố thông tin mạng để khắc phục, hạn chế những tác động xấu do sự cố gây ra ảnh hưởng đến bản thân và nhà trường.

4. Bộ phận công nghệ thông tin

Thường xuyên cập nhật và thông tin cảnh báo về các nguy cơ, lỗ hổng bảo mật an toàn thông tin mạng của ngành, của các cơ quan chức năng để kiểm tra, rà soát, phối hợp xử lý, khắc phục các lỗ hổng, điểm yếu về bảo mật, an toàn thông tin đối với các hệ thống thông tin do nhà trường chủ trì xây dựng hoặc thuê dịch vụ công nghệ thông tin và các hệ thống do ngành giáo dục quản lý vận hành.

Tham gia tập huấn, huấn luyện, diễn tập nâng cao trình độ, kỹ năng, năng lực giám sát an toàn thông tin mạng và tham mưu tổ chức tuyên truyền, tập huấn nâng cao nhận thức, kiến thức an toàn thông tin cho viên chức, người lao động và học sinh trong nhà trường.

Thường xuyên rà soát, kiểm tra, phối hợp xử lý, khắc phục các lỗ hổng, điểm yếu về bảo mật, an toàn thông tin đối với hệ thống thông tin trong nhà trường. Chủ trì xây dựng hoặc thuê dịch vụ công nghệ thông tin và các hệ thống thông tin do nhà quản lý vận hành.

3. Các tổ chuyên môn

Phối hợp đẩy mạnh công tác truyền thông, nâng cao nhận thức, kỹ năng số, kỹ năng khai thác thông tin an toàn trên môi trường mạng trong đội ngũ giáo viên, nhân viên của tổ.

Theo dõi, giám sát việc khai thác thông tin trên không gian mạng, thường xuyên quán triệt trách nhiệm bản thân trong việc thực hiện tốt văn hóa giao tiếp và khai thác thông tin trên không gian mạng.

Trên đây là Kế hoạch ứng phó sự cố và đảm bảo an toàn thông tin của Trường PTDTBT tiểu học Mường Anh. Yêu cầu các tổ chức đoàn thể, giáo viên, nhân viên nghiêm túc thực hiện kế hoạch. Trong quá trình tổ chức thực hiện, trường hợp phát sinh vướng mắc, kịp thời báo cáo về nhà trường để tổng hợp, xem xét, chỉ đạo giải quyết theo quy định./.

Nơi nhận:
- Phòng GD&ĐT (b/c);
- Các tổ CM, Tổ CNTT;
- Lưu VT.

P. HIỆU TRƯỞNG

Nguyễn Thị Nga