UBND TỈNH QUẢNG NGÃI **SỞ GIÁO DỤC VÀ ĐÀO TẠO**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 4338 /QĐ-SGDĐT	*Quảng Ngãi, ngày 23 tháng 12 năm 2022*

QUYẾT ĐỊNH

Phê duyệt Phương án Ứng phó sự cố, bảo đảm an toàn thông tin đối với Hệ thống thông tin Sở Giáo dục và Đào tạo tỉnh Quảng Ngãi

GIÁM ĐỐC SỞ GIÁO DỤC VÀ ĐÀO TẠO

Căn cứ Luật An ninh mạng ngày 12/6/2018;

Căn cứ Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ Quy định chi tiết một số điều của 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 131/QĐ-TTg ngày 25/01/2022 của Thủ tướng Chính phủ về phê duyệt Đề án "Tăng cường ứng dụng công nghệ thông tin và chuyển đổi số trong giáo dục và đào tạo giai đoạn 2022-2025, định hướng đến năm 2030";

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông Quy định chi tiết và hướng dẫn một số điều của 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;

Căn cứ Quyết định số 1571/QĐ-UBND ngày 28/10/2019 của UBND tỉnh Quảng Ngãi về việc Ban hành Kế hoạch Ứng phó sự cố, bảo đảm an toàn, an ninh thông tin mạng trên địa bàn tỉnh Quảng Ngãi giai đoạn 2020-2025; Kế hoạch số 166/KH-UBND ngày 14/10/2022 của Chủ tịch UBND tỉnh Quảng Ngãi về Tăng cường đảm bảo an toàn, an ninh thông tin trong hoạt động các cơ quan nhà nước tỉnh Quảng Ngãi đến năm 2025 và định hướng đến năm 2030; Công văn số 5609/UBND-KGVX ngày 03/11/2022 của Chủ tịch UBND tỉnh Quảng Ngãi về việc triển khai thực hiện Chỉ thị số 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ;

Căn cứ Quyết định số 146/QĐ-STTTT ngày 03/11/2021 của Sở Thông tin và Truyền thông tỉnh Quảng Ngãi về việc Phê duyệt cấp độ an toàn hệ thống thông tin đối với Hệ thống thông tin Sở Giáo dục và Đào tạo tỉnh Quảng Ngãi;

Căn cứ Quyết định số 38/2021/QĐ-UBND ngày 19/8/2021 của UBND tỉnh Quảng Ngãi về ban hành Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Giáo dục và Đào tạo tỉnh Quảng Ngãi;

Theo đề nghị của Chánh Văn phòng Sở Giáo dục và Đào tạo,

QUYẾT ĐỊNH:

Điều 1. Phê duyệt Phương án Ứng phó sự cố, bảo đảm an toàn thông tin đối với Hệ thống thông tin Sở Giáo dục và Đào tạo tỉnh Quảng Ngãi *(có Phương án kèm theo)*.

Điều 2. Phương án Ứng phó sự cố, bảo đảm an toàn thông tin đối với Hệ thống thông tin Sở Giáo dục và Đào tạo là căn cứ để Lãnh đạo Sở, Trưởng các phòng thuộc Sở chủ động chỉ đạo, điều hành các hoạt động ứng phó sự cố, bảo đảm an toàn thông tin mạng, hạn chế thấp nhất thiệt hại do sự cố mất an toàn, an ninh thông tin gây ra đối với Hệ thống thông tin Sở Giáo dục và Đào tạo, đơn vị, cơ sở giáo dục liên quan.

Điều 3. Quyết định này có hiệu lực kể từ ngày ký.

Điều 4. Chánh Văn phòng Sở, Chánh Thanh tra Sở, Trưởng các thuộc Sở, Thủ trưởng các đơn vị thuộc Sở và các đơn vị, cơ sở giáo dục liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 4;
- Cục CNTT, Bộ GDĐT (báo cáo);
- UBND tỉnh (báo cáo);
- Sở Thông tin và Truyền thông;
- Lãnh đạo Sở GDĐT;
- Các phòng thuộc Sở GDĐT;
- Đơn vị trực thuộc Sở GDĐT;
- Phòng GDĐT huyện, thị xã, thành phố;
- Trung tâm GDNN-GDTX huyện, thị xã;
- Lưu: VT, VP, ndh.

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ GIÁO DỤC VÀ ĐÀO TẠO
TỈNH QUẢNG NGÃI

Ký bởi: Sở Giáo dục và Đào tạo
Email: sgd@quangngai.gov.vn
Cơ quan: Ủy ban Nhân dân tỉnh Quảng Ngãi
Thời gian ký: 23/12/2022 08:12:26

Nguyễn Ngọc Thái

UBND TỈNH QUẢNG NGÃI
SỞ GIÁO DỤC VÀ ĐÀO TẠO

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

PHƯƠNG ÁN
Ứng phó sự cố, bảo đảm an toàn thông tin đối với Hệ thống thông tin Sở Giáo dục và Đào tạo tỉnh Quảng Ngãi
(Kèm theo Quyết định số: 4338/QĐ-SGDĐT ngày 23 /12/2022 của Giám đốc Sở Giáo dục và Đào tạo)

I. MỤC ĐÍCH, YÊU CẦU

1. Phương án này hướng dẫn việc ứng cứu sự cố hệ thống thông tin, trách nhiệm của các phòng chuyên môn và cá nhân có liên quan đến đảm bảo an toàn, an ninh thông tin đối với Hệ thống thông tin Sở Giáo dục và Đào tạo, đơn vị, cơ sở giáo dục liên quan.

2. Luôn quán triệt và thực hiện có hiệu quả phương châm chủ động thực hiện săn lùng mối nguy hại và rà quét lỗ hổng hệ thống thông tin trong phạm vi quản lý nhằm phòng ngừa, chủ động, ứng phó kịp thời, khắc phục khẩn trương và hiệu quả các sự cố xảy ra.

3. Nâng cao năng lực xử lý tình huống sự cố, mất an toàn thông tin của công chức, viên chức và người lao động đối với các đơn vị, cơ sở giáo dục liên quan.

4. Tăng cường thông tin, tuyên truyền, cảnh báo, hướng dẫn các biện pháp phòng, tránh ứng phó sự cố hệ thống thông tin nhằm phát huy ý thức tự giác, chủ động ứng phó của cán bộ, công chức, viên chức và người lao động trong ngành giáo dục.

II. NHIỆM VỤ TRỌNG TÂM

1. Văn phòng Sở chịu trách nhiệm trước Giám đốc Sở trong việc ứng cứu sự cố, an toàn thông tin của Sở, như sau:

Tham mưu Sở tổ chức triển khai, hướng dẫn, kiểm tra, đôn đốc việc thực hiện phương án này.

Chủ trì, phối hợp với các phòng, cơ quan, đơn vị thuộc Sở thường xuyên kiểm tra, đề xuất Giám đốc Sở công tác bảo đảm an toàn thông tin mạng định kỳ, hàng năm hoặc theo hướng dẫn của cơ quan chuyên môn.

Cử công chức tham gia hoạt động ứng cứu sự cố nhằm bảo đảm an toàn thông tin mạng khi có đề nghị từ các phòng, cơ quan, đơn vị trực thuộc.

2. Các phòng thuộc Sở trong phạm vi nhiệm vụ, quyền hạn, có trách nhiệm phối hợp với Văn phòng Sở trong quá trình tham gia ứng cứu sự cố an toàn thông tin khi xảy ra sự cố.

3. Các cơ quan, đơn vị trực thuộc Sở, cơ sở giáo dục liên quan căn cứ chức năng, nhiệm vụ quyền hạn được giao phân công công chức, viên chức và người lao động của đơn vị thực hiện công tác đảm bảo an toàn, an ninh thông tin tại đơn vị; Xây dựng đề xuất cấp độ an toàn hệ thống thông tin đối với các hệ thống thông tin của các cơ quan, đơn vị theo quy định. Căn cứ Phương án này, ban hành Phương án ứng Ứng phó sự cố, bảo đảm an toàn thông tin đối với Hệ thống thông tin của cơ quan, đơn vị.

III. BIỆN PHÁP THỰC HIỆN

1. Biện pháp phòng ngừa sự cố hệ thống thông tin

1.1 Về thông tin, tuyên truyền

Trưởng các phòng thuộc Sở, Thủ trưởng các cơ quan, đơn vị giáo dục tăng cường công tác tuyên truyền đến công chức, viên chức và người lao động nâng cao ý thức trách nhiệm về đảm bảo an toàn thông tin. Nội dung tuyên truyền về an toàn, an ninh thông tin, các văn bản, quy định hiện hành, như: Luật An toàn thông tin mạng, 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; Quyết định số 1017/QĐ-TTg ngày 14/8/2018 của Thủ tướng Chính phủ phê duyệt Đề án giám sát an toàn thông tin mạng đối với hệ thống, dịch vụ công nghệ thông tin phục vụ Chính phủ điện tử đến năm 2020, định hướng đến năm 2025; 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; Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông Quy định chi tiết và hướng dẫn một số điều của 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 44/2012/QĐ-UBND ngày 20/10/2015 của UBND tỉnh Quảng Ngãi về việc ban hành Quy chế bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan, đơn vị quản lý nhà nước tỉnh Quảng Ngãi; Kế hoạch số 166/KH-UBND ngày 14/10/2022 của UBND tỉnh về tăng cường đảm bảo an toàn, an ninh thông tin trong hoạt động các cơ quan nhà nước tỉnh Quảng Ngãi đến năm 2025 và định hướng đến năm 2030 và các văn bản quy phạm pháp luật về an toàn thông tin mạng và các văn bản, tài liệu hướng dẫn chuyên môn về an toàn thông tin mạng.

1.2 Nhận diện các nguy cơ, sự cố, mất an toàn hệ thống thông tin

Các nguy cơ, sự cố có khả năng ảnh hưởng đến hệ thống thông tin đối với Hệ thống thông tin Sở Giáo dục và Đào tạo, cơ quan, đơn vị, cơ sở giáo dục, như sau:

+ Sự cố do bị tấn công mạng: 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 từ chối dịch vụ; Tấn công giả mạo; 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.

+ 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 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.

+ Sự cố liên quan đến các thảm họa thiên tai: Bão, lụt, gió lốc, động đất, sấm sét, hỏa hoạn,...

1.3 Phòng chống virus máy tính, bảo mật cơ sở dữ liệu và an ninh mạng

Bảo mật số liệu: Công chức, viên chức và người lao động có trách nhiệm bảo mật số liệu nghiệp vụ trên máy tính. Tuyệt đối không chia sẻ thư mục, dữ liệu cá nhân trên hệ thống mạng LAN cơ quan. Việc chia sẻ dữ liệu trên mạng do công chức quản trị mạng Sở thực hiện theo quyết định của Lãnh đạo Sở và theo phân cấp sử dụng tài nguyên mạng.

Bảo mật truy cập: Các chương trình, phần mềm được được bàn giao cho công chức, viên chức và người lao động sử dụng phải được thiết lập mật khẩu theo quy định. Kịp thời điều chỉnh vị trí công tác cho người sử dụng (khi có sự thay đổi); xóa, đóng khỏi hệ thống các tài khoản người dùng đã nghỉ việc, nghỉ hưu, chuyển công tác.

Bảo mật hệ thống mạng và truyền tin: Mạng và đường truyền được áp dụng các chế độ bảo mật cần thiết, chống xâm nhập bất hợp pháp. Công chức quản trị mạng có trách nhiệm thường xuyên theo dõi, kiểm tra phát hiện kịp thời các hoạt động xâm nhập và có biện pháp xử lý kịp thời.

An toàn trong sử dụng: Khi không làm việc với máy vi tính trong thời gian dài, công chức, người lao động tại các phòng chuyên môn thuộc Sở phải tắt máy tính hoặc đặt chế độ bảo vệ để đảm bảo an toàn cho dữ liệu của cá nhân.

Phòng, chống virus: Công chức, người lao động tại các phòng chuyên môn thuộc Sở có trách nhiệm tuân thủ các biện pháp, tài liệu hướng dẫn về cảnh báo về lỗ hổng bảo, cảnh báo nguy cơ tấn công theo tài liệu hướng dẫn của cơ quan có thẩm quyền nhằm rà soát, giám sát, ngăn chặn, phòng ngừa, xử lý kịp thời hạn chế đến mức thấp nhất nguy cơ gây mất an toàn an ninh thông tin. Mọi dữ liệu từ các thiết bị lưu trữ bên ngoài *(USB, ổ cứng di động, thẻ nhớ,...)* đều phải được quét, diệt virus trước khi sao chép vào máy. Những máy tính phát hiện có virus phải được báo cáo ngày cho công chức quản trị mạng và tách khỏi mạng về mặt vật lý để tránh tình trạng lây nhiễm sang các máy tính khác. Không truy cập vào các trang website, đường dẫn liên kết không rõ ràng; không truy

cập vào các link hoặc tải về các file tài liệu từ các địa chỉ thư không nắm rõ thông tin, địa chỉ người gửi.

1.4 Kiểm soát việc cài đặt các phần mềm và thực hiện cơ chế sao lưu, phục hồi

Kiểm soát chặt chẽ việc cài đặt các phần mềm mới lên máy chủ, máy trạm: Các phần mềm được cài đặt trên máy chủ, máy trạm (*bao gồm hệ điều hành, các phần mềm ứng dụng văn phòng, phần mềm phục vụ công việc, tiện ích khác)* phải được thường xuyên theo dõi, cập nhật bản vá lỗi bảo mật của nhà phát triển, lựa chọn cài đặt các phần mềm chống, diệt virus, mã độc và thường xuyên cập nhật phiên bản mới, đặt lịch quét virus theo định kỳ.

Cơ chế sao lưu, phục hồi máy chủ, máy trạm: Công chức, người lao động phải thực hiện việc sao lưu định kỳ cơ sở dữ liệu và các dữ liệu quan trọng khác *(bao gồm dữ liệu phát sinh trong quá trình vận hành các phần mềm ứng dụng như: các tập tin văn bản, hình ảnh,…)* vào các thiết bị lưu trữ bên ngoài *(USB, ổ cứng di động, thẻ nhớ,...)* nhằm phục vụ cho việc phục hồi, khắc phục dữ liệu kịp thời khi có sự cố xảy ra.

1.5 Đảm bảo an toàn hệ thống thông tin mạng LAN cơ quan

Về cơ sở hạ tầng: Đảm bảo việc lắp đặt thiết bị chống sét, thiết bị cảnh báo phòng chống cháy, nổ tại trụ sở để bảo vệ hệ thống, thiết bị công nghệ thông tin.

Quản lý hệ thống mạng nội bộ: Mạng nội bộ của Sở khi kết nối với mạng Internet phải thông qua thiết bị tường lửa Sophos do Sở Thông tin và Truyền thông Quảng Ngãi lắp đặt để kiểm soát, hạn chế việc truy cập trái phép từ bên ngoài. Các máy chủ, máy trạm trên hệ thống phải được cài đặt phần mềm diệt virus có bản quyền.

Quản lý hệ thống mạng không dây (wifi): Khi thiết lập mạng không dây có kết nối vào mạng nội bộ phải thiết lập các thông số cần thiết như định danh, mật mã, mã hóa dữ liệu, có thay đổi mật mã định kỳ.

Quản lý truy cập từ xa vào mạng nội bộ: Đối với việc truy cập từ xa vào mạng nội bộ phải được theo dõi, quản lý chặt chẽ, nhất là truy cập có sử dụng chức năng quản trị, phải thiết lập mật mã độ an toàn cao, thường xuyên thay đổi mật mã, hạn chế truy cập từ xa vào mạng nội bộ từ các điểm truy cập Internet công cộng.

1.6 Đảm bảo an ninh, an toàn trong dạy và học trực tuyến

Thủ trưởng các cơ sở giáo dục có trách nhiệm quản lý và tổ chức thực hiện các hoạt động chuyên môn và các biện pháp đảm bảo an ninh, an toàn trong dạy - học theo hình thức trực tuyến. Lựa chọn hệ thống quản lý và phần mềm dùng để dạy – học, kiểm tra, đánh giá trực tuyến và tập huấn cho người sử dụng về các biện pháp đảm bảo an ninh, an toàn.

Thủ trưởng các cơ sở giáo dục cần thường xuyên kiểm tra và chủ động phối hợp với các cơ quan chức năng ở địa phương để phòng chống tội phạm,

bạo lực học đường trên môi trường mạng. Ngay khi phát hiện tình huống mất an ninh, an toàn trong dạy và học theo hình thức trực tuyến, cơ sở giáo dục phải chủ động xử lý hoặc kiến nghị các cơ quan có thẩm quyền xử lý.

Nhà giáo chịu trách nhiệm về nội dung bài giảng, học liệu, phương pháp; đồng thời, thông tin đầy đủ về thời khóa biểu và hướng dẫn người học sử dụng hệ thống phần mềm dạy học trực tuyến. Nhà giáo kiểm soát tài khoản người học, sự tham gia và đánh giá chất lượng học tập của người học đúng quy định. Khi phát hiện tình huống mất an ninh, an toàn trong dạy và học theo hình thức trực tuyến, Nhà giáo cần kịp thời báo cáo Thủ trưởng cơ sở giáo dục.

Người học phải dùng tên thật, tuyệt đối không bình luận hay có các hành vi khác làm ảnh hưởng tới lớp học. Người học chịu trách nhiệm bảo vệ tài khoản cá nhân; tuyệt đối không chia sẻ tài khoản và mật khẩu lớp học cho người khác. Khi phát hiện có người lạ tham gia lớp học hoặc phát hiện tình huống mất an ninh, an toàn trong dạy và học theo hình thức trực tuyến phải thông báo ngay cho nhà giáo phụ trách lớp học, cha mẹ để có biện pháp xử lý.

V. PHÂN CÔNG THỰC HIỆN

1. Trách nhiệm của Trưởng các phòng thuộc Sở

Thường xuyên chỉ đạo công chức, viên chức và người lao động thực hiện nghiêm các quy định bảo đảm an toàn thông tin hệ thống mạng LAN cơ quan.

Phối hợp với Văn phòng Sở trong công tác kiểm tra, phát hiện, xử lý kịp thời các sự cố về an toàn thông tin mạng.

2. Trách nhiệm của công chức, viên chức và người lao động tại các phòng thuộc Sở

Có trách nhiệm quản lý tài khoản, mật khẩu đăng nhập vào các phần mềm dùng chung được triển khai tại Sở; thực hiện nghiêm các quy định về đảm bảo an toàn thông tin trong hệ thống mạng LAN cơ quan Văn phòng Sở. Thường xuyên thay đổi mật khẩu đủ mạnh *(ít nhất 8 ký tự, có chữ hoa, chữ thường, số, ký tự đặc biệt)* để đảm bảo an toàn, an ninh thông tin.

Thực hiện tiếp nhận, xử lý, phát hành, quản lý và lưu trữ văn bản, hồ sơ điện tử trên phần mềm quản lý văn bản đúng quy định trên môi trường mạng và ký số cá nhân, đảm bảo theo đúng quy định pháp luật hiện hành. Phải sử dụng thư điện tử công vụ để gửi, nhận văn bản giữa các cơ quan nhà nước.

Không được tự ý cài đặt phần mềm, tải trên mạng khi chưa có sự đồng ý, hướng dẫn của Văn phòng Sở hoặc tự gỡ bỏ phần mềm diệt virus, an toàn mạng đã được cài đặt trên máy trạm.

Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm virus, nhiễm mã độc trên máy trạm *(máy hoạt động chậm bất thường, cảnh báo từ phần mềm diệt virus, mất dữ liệu,...)*, người sử dụng phải báo ngay cho cán bộ quản trị mạng cơ quan để phối hợp xử lý kịp thời tránh lây lan đến các máy trạm khác.

3. Trách nhiệm của công chức quản trị mạng

Làm đầu mối ứng cứu sự cố đối với hệ thống mạng LAN cơ quan theo đúng quy trình ứng cứu sự cố dựa trên tính chất, mức độ, phạm vi và nguyên nhân xảy ra sự cố; bảo đảm nhanh chóng, chính xác, kịp thời, an toàn và hiệu quả.

Phối hợp với các cơ quan, đơn vị có liên quan kiểm tra, rà soát đánh giá an toàn thông tin thường xuyên, định kỳ hoặc đột xuất khi có các yếu tố quan trọng, đặc biệt thay đổi để kịp thời phát hiện các lỗ hổng đang tồn tại, các nguy cơ mất an toàn thông tin mạng.

Thực hiện phân quyền truy cập và hướng dẫn sử dụng cho công chức, viên chức và người lao động sử dụng các phần mềm dùng chung của tỉnh đang triển khai tại Sở *(như Phần mềm Quản lý văn bản và điều hành - Office; Hệ thống thông tin giải quyết thủ tục hành chính tỉnh Quảng Ngãi – iGate 2.0; Hệ thống thông tin báo cáo Bộ, ngành, địa phương,...)*; kịp thời điều chỉnh vị trí công tác cho người sử dụng *(khi có sự thay đổi)*; xóa khỏi hệ thống các tài khoản người dùng đã nghỉ hưu, chuyển công tác, thôi việc.

Chịu trách nhiệm quản lý các tài khoản quản trị được bàn giao và thường xuyên thay đổi mật khẩu quản trị đủ mạnh để đảm bảo an toàn, bảo mật thông tin. Mật khẩu có ít nhất 8 ký tự, có chữ hoa, chữ thường, số, ký tự đặc biệt, tránh nguy cơ mất an toàn an ninh thông tin.

Phối hợp với Văn phòng UBND tỉnh, Sở Thông tin và Truyền thông, Trung tâm Phục vụ hành chính công tỉnh, Cục Công nghệ thông tin Bộ GDĐT và các cơ quan, đơn vị có liên quan thực hiện khắc phục kịp thời các lỗi phát sinh của các phần mềm (nếu có) khi có phản ánh, yêu cầu.

Chủ động thực hiện săn lùng mối nguy hại và rà quét lỗ hổng hệ thống thông tin trong phạm vi quản lý tối thiểu 01 lần/6 tháng.

Tham mưu các văn bản liên quan đến ký số, cấp mới, thu hồi, gia hạn chứng thư số đơn vị, cá nhân theo quy định, phải đảm bảo an toàn thông tin *(chú ý mật khẩu bảo mật)*.

Tham mưu việc sửa chữa, bảo trì, cài đặt các thiết bị, phần mềm bảo mật tại các máy tính thuộc các phòng chuyên môn thuộc Sở tránh nguy cơ mất an toàn, an ninh thông tin máy trạm người dùng.

Tham mưu, phối hợp việc cử công chức, viên chức và người lao động tham dự các lớp kỹ năng bảo vệ hệ thống thông tin do Bộ GDĐT, Sở Thông tin và Truyền thông, các cơ quan liên quan tổ chức.

4. Trách nhiệm của đơn vị trực thuộc Sở, cơ sở giáo dục liên quan

Phân công lãnh đạo và cán bộ, viên chức phụ trách đảm bảo an toàn ứng dụng công nghệ thông tin và chuyển đổi số của cơ quan, đơn vị.

Thường xuyên theo dõi an toàn thông tin, có biện pháp ứng phó sự cố, đảm bảo an toàn thông tin cho cơ quan, đơn vị.

5. Phương án ứng phó sự cố an toàn hệ thống thông tin

Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm virus, nhiễm mã độc trên máy trạm *(máy hoạt động chậm bất thường, cảnh báo từ phần mềm diệt virus, mất dữ liệu,...)*, công chức, viên chức và người lao động thực hiện các bước như sau:

Bước 1. Khoanh vùng cô lập sự cố

- Sau khi phát hiện sự cố, công chức, viên chức và người lao thực hiện khoanh vùng cô lập máy tính bị sự cố, như: ngắt kết nối máy tính khỏi hệ thống thông tin mạng LAN của cơ quan *(tắt máy, rút dây mạng,...)*.

- Báo cáo ngay Lãnh đạo phòng, đơn vị các dấu hiệu sự cố; đồng thời thông báo kịp thời về Văn phòng Sở để cử công chức Quản trị mạng phối hợp kiểm tra, xử lý.

Bước 2. Thu thập thông tin phục vụ phân tích sự cố:

- Công chức quản trị mạng Sở phối hợp với công chức, người lao động tại phòng chuyên môn thuộc Sở, đơn vị, kiểm tra máy tính đang bị sự cố để nắm bắt thông tin ban đầu về sự cố.

- Các thông tin thu thập gồm: Thông tin hệ thống; chức năng của hệ thống; cấu hình của hệ thống *(OS, servise, version, network,...)*; Thu thập chứng cứ; Thu thập bộ nhớ; Thu thập trạng thái network và các kết nối; Thu thập các tiến trình đang chạy; Thu thập hard drive media; Thu thập removeble media; Thu thập Log file,…

Bước 3. Phân tích sự cố:

- Công chức quản trị mạng phối hợp với công chức, viên chức và người lao động kiểm tra máy tính đang bị sự cố để phân tích nguyên nhân ban đầu về sự cố.

- Các thông tin phân tích gồm: Phân tích dòng thời gian; Thời gian bị sửa đổi, truy cập, tạo hoặc thay đổi; Thời gian thực hiện các cập nhật lớn đối với hệ thống; Thời điểm mà hệ thống sử dụng lần cuối cùng; Phân tích dữ liệu; Kiểm tra sự thay đổi cấu hình; Kiểm tra hệ thống tập tin có bị mã độc; Kiểm tra tập tin Internet history và các tập tin history khác; Kiểm tra Registry và tiến trình; Quan sát các tập tin, tiến trình lúc khởi động; Phân tích log file.

Bước 4. Xử lý sự cố:

- Trường hợp sự cố có khả năng kiểm soát, xử lý được: Công chức quản trị mạng tiến hành xử lý sự cố bao gồm các bước: Gỡ bỏ sự cố; Xác định và gỡ bỏ các backdoors; Phân tích và kiểm tra lỗ hổng sau khi thực hiện các bản vá lỗi; Khôi phục dữ liệu; Thu thập các tập tin, hình ảnh, email,… bị xóa, thời gian bị xóa; Tìm kiếm các tập tin không thể khôi phục; Khôi phục các tập tin phù hợp.

- Trường hợp sự cố ngoài khả năng kiểm soát, xử lý được (sự cố có tính chất nghiêm trọng): triển khai ngay các biện pháp xử lý ngăn chặn tấn công tránh lây nhiễm sự cố các máy tính khác trên hệ thống thông tin và tham mưu

văn bản báo cáo, đề nghị Sở Thông tin và Truyền thông, Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Quảng Ngãi, các đơn liên quan để có các biện pháp hỗ trợ, xử lý kịp thời.

Bước 5. Tổng hợp báo cáo:

- Sau khi triển khai các giải pháp ứng cứu sự cố, công chức quản trị mạng tham mưu, tổ chức họp phân tích nguyên nhân, rút kinh nghiệm trong hoạt động xử lý sự cố và đề xuất các biện pháp ứng cứu cho các sự cố tương tự.

- Tham mưu báo cáo kết quả ứng cứu sự cố xảy ra về cơ quan chủ quản, Sở Thông tin và Truyền thông, Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Quảng Ngãi để biết, theo dõi.

Bước 6. Lưu hồ sơ:

Toàn bộ các hồ sơ trong quá trình xử lý sự cố, công chức quản trị mạng lưu trữ phục vụ các hoạt động quản lý và theo dõi, kiểm tra định kỳ.

VI. TỔ CHỨC THỰC HIỆN

1. Các phòng, đơn vị trực thuộc Sở cần nổ lực tổ chức phối hợp đồng bộ nhằm đưa công tác phòng ngừa, ứng phó sự cố an ninh thông tin hiệu quả; Tổ chức săn lùng mối nguy hại và rà quét lỗ hổng hệ thống thông tin trong phạm vi quản lý theo quy định.

2. Các phòng thuộc Sở trong phạm vi nhiệm vụ, quyền hạn có trách nhiệm phối hợp với Văn phòng Sở trong quá trình tham gia ứng cứu sự cố an toàn thông tin khi xảy ra sự cố.

3. Các cơ quan, đơn vị trực thuộc Sở căn cứ chức năng, nhiệm vụ quyền hạn được giao phân công công chức, viên chức và người lao động của đơn vị thực hiện công tác đảm bảo an toàn, an ninh thông tin tại đơn vị; Xây dựng hồ sơ đề xuất cấp độ an toàn hệ thống thông tin đối với các hệ thống thông tin của các cơ quan, đơn vị theo quy định. Ban hành Phương án ứng Ứng phó sự cố, bảo đảm an toàn thông tin đối với Hệ thống thông tin của cơ quan, đơn vị để triển khai thực hiện.

4. Phương án này được phổ biến đến toàn thể công chức, viên chức và người lao động ngành giáo dục biết để thực hiện. Trong quá trình thực hiện nếu có vướng mắc và cần sửa đổi, bổ sung, đề nghị các cơ quan, đơn vị, cá nhân kịp thời phản ánh về Văn phòng Sở Giáo dục và Đào tạo để tổng hợp, tham mưu, sửa đổi, bổ sung kịp thời./.