UBND TỈNH BÌNH PHƯỚC **SỞ XÂY DỰNG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 1464 /KH-SXD	*Bình Phước, ngày 29 tháng 5 năm 2024*

KẾ HOẠCH
Ứng phó sự cố và đảm bảo an toàn hệ thống thông tin của Sở Xây dựng

Căn cứ Công văn số 1552/TBATANM ngày 26/4/2024 của Tiểu ban an toàn an ninh mạng về Tăng cường công tác bảo đảm an ninh mạng.

Sở Xây dựng ban hành Kế hoạch ứng phó sự cố và đảm bảo an toàn thông tin trong hoạt động cơ quan như sau:

I. MỤC ĐÍCH YÊU CẦU

1. Mục đích

- Nhằm tạo chuyển biến mạnh mẽ trong nhận thức về an toàn thông tin, đưa ra các giải pháp ứng phó khi gặp sự cố mất an toàn hệ thống thông tin mạng.

- Đảm bảo an toàn hệ thống thông tin mạng trong hoạt động của cơ quan, có khả năng thích ứng một cách chủ động, linh hoạt và giảm thiểu các nguy cơ, đe dọa mất an toàn hệ thống thông tin mạng.

- Nâng cao nhận thức về an toàn thông tin trên hệ thống mạng cho đội ngũ công chức, viên chức và người lao động của Sở.

- Đảm bảo các nguồn lực và các điều kiện cần thiết để sẵn sàng triển khai kịp thời, hiệu quả phương án ứng phó sự cố bảo đảm an toàn thông tin mạng.

2. Yêu cầu

- 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 Sở Thông tin và Truyền thông trong quá trình triển khai thực hiện để được hỗ trợ khi cần thiết. 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 hệ thống thông tin mạng trong hoạt động của cơ quan.

- Thường xuyên trao đổi thông tin, chia sẻ kinh nghiệm trong công tác đảm bảo an toàn thông tin giữa các cơ quan nhà nước trên địa bàn tỉnh; phối hợp, hỗ trợ với các đơn vị liên quan.

II. NỘI DUNG THỰC HIỆN

1. Triển khai các hoạt động khi chưa có sự cố xảy ra

- Tổ chức tuyên truyền, phổ biến, hướng dẫn các nội dụng của Luật An toàn thông tin 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; 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 và định hướng đến năm 2025.

- Đánh giá hiện trạng và khả năng bảo đảm an toàn thông tin mạng của hệ thống thông tin (mạng LAN) của đơn vị; Đánh giá, dự báo các nguy cơ, sự cố, tấn công mạng có thể xảy ra với của hệ thống thông tin (mạng LAN); Đánh giá, dự báo các hậu quả, thiệt hại, tác động có thể có nếu xảy ra sự cố; đánh giá về hiện trạng phương tiện, trang thiết bị, công cụ hỗ trợ, nhân lực, vật lực phục vụ đối phó, ứng cứu, khắc phục sự cố.

- Đầu tư, quản lý, khai thác sử dụng hiệu quả các trang thiết bị thiết yếu bảo đảm an toàn thông tin cho cơ quan, đơn vị gồm: Thiết bị tường lửa mạng, thiết bị phục vụ quản trị, giám sát an ninh mạng…

- Sử dụng phần mềm virus có bản quyền đáp ứng yêu cầu bảo vệ máy tính cho 100% máy tính trong mạng nội bộ của cơ quan, đơn vị theo hướng ưu tiên sử dụng phần mềm virus Cyrada,…

- Cử công chức, viên chức tham gia các lớp tập huấn về ứng phó sự cố, đảm bảo an toàn thông tin mạng.

- Thường xuyên theo dõi, giám sát hệ thống thông tin mạng nội bộ của Sở, kịp thời phát hiện sự cố mất an toàn và cập nhật các bản vá lỗi cho hệ thống.

- Đơn vị thực hiện: Văn phòng Sở.

- Đơn vị phối hợp: Các phòng, đơn vị trực thuộc Sở.

- Thời gian thực hiện: Thường xuyên trong năm.

2. Triển khai các hoạt động khi có sự cố xảy ra

- Tiếp nhận, phân tích, ứng cứu ban đầu và thông báo sự cố: Thường xuyên theo dõi, 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, mạng xã hội...; phát hiện sự cố thông qua kiểm tra, rà soát, đánh giá) và thông báo đến cơ quan chuyên môn có liên quan để phối hợp xử lý sự cố.

- Triển khai ứng cứu, ngăn chặn và xử lý sự cố: Triển khai phân tích, xác định tình hình sự cố để xác định phạm vi ảnh hưởng, nguồn gốc tấn công để tổ chức ứng cứu ngăn chặn, giảm thiểu tác động, thiệt hại đến hệ thống thông tin.

- Khắc phục, gỡ bỏ và khôi phục 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 của hệ thống thông tin. Khôi phục hệ thống, dữ liệu kết nối và kiểm tra thử toàn bộ hệ thống sau khi khắc phục sự cố.

- **Tổng kết, đánh giá hệ thống thông tin:** Tổ chức triển khai kiểm tra,

đánh giá hoạt động của toàn bộ hệ thống thông tin, 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.

- Đơn vị thực hiện: Văn phòng Sở.

- Đơn vị phối hợp: Các phòng, đơn vị trực thuộc Sở.

- Thời gian thực hiện: Khi có sự cố xảy ra**.**

III. TỔ CHỨC THỰC HIỆN

1. Văn phòng Sở phối hợp các phòng, đơn vị tham mưu lãnh đạo tổ chức triển khai phổ biến Kế hoạch ứng phó sự cố, bảo đảm an toàn thông tin mạng của Sở Xây dựng trên cổng thông tin điện tử, bảo đảm đúng tiến độ, chất lượng, hiệu quả, tránh hình thức.

2. Thực hiện bố trí công chức đảm bảo an toàn thông tin của Sở Xây dựng; kịp thời thông báo về Sở Thông tin và Truyền thông khi có sự cố xảy ra ảnh hưởng đến an toàn thông tin mạng của Sở Xây dựng.

3. Kinh phí thực hiện Kế hoạch ứng phó sự cố, bảo đảm an toàn thông tin mạng do cơ quan đảm bảo.

Trên đây là Kế hoạch ứng phó sự cố và đảm bảo an toàn thông tin mạng của Sở Sở Xây dựng. Giám đốc Sở yêu cầu các phòng, đơn vị trực thuộc nghiêm túc triển khai thực hiện Kế hoạch này.Trong quá trình thực hiện, nếu có khó khăn, vướng mắc, các đơn vị phản ánh trực tiếp về Văn phòng Sở Xây dựng để tổng hợp trình Giám đốc xem xét, quyết định./.

Nơi nhận:
- Các phòng, đơn vị trực thuộc;
- Lãnh đạo Sở;
- Lưu VT.

GIÁM ĐỐC

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ XÂY DỰNG
NINH BÌNH PHƯỚC

Võ Tất Dũng