UBND TỈNH TUYÊN QUANG
SỞ TƯ PHÁP

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

Số: 111 /KH-STP

Tuyên Quang, ngày 25 tháng11 năm 2023

KẾ HOẠCH
Ứng phó sự cố bảo đảm an toàn thông tin mạng của Sở Tư pháp tỉnh Tuyên Quang

Sở Tư pháp tỉnh Tuyên Quang xây dựng Kế hoạch Ứng dụng phó sự cố bảo đảm an toàn thông tin mạng, như sau:

I. MỤC ĐÍCH YÊU CẦU

1. Mục đích

- 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 thông tin mạng.

- Đảm bảo nhân lực, kinh phí và các điều kiện cần thiết khác để sẵn sàng triển khai kịp thời, hiệu quả phương án ứng cứu sự cố, bảo đảm an toàn thông tin mạng; có khả năng thích ứng chủ động, linh hoạt và giảm thiểu các nguy cơ mất an toàn thông tin mạng.

2. Yêu cầu

- Khảo sát, đánh giá các nguy cơ, sự cố an toàn thông tin mạng toàn bộ hệ thống thông tin của Sở Tư pháp để nhanh chóng xác định được tính chất, mức độ nghiêm trọng của sự cố khi có sự cố xảy ra; đưa ra được các phương án đối phó, ứng cứu sự cố kịp thời, chính xác.

- Có sự phối hợp chặt chẽ giữa Sở Tư pháp với Sở Thông tin và truyền thông và các cơ quan, đơn vị có liên quan; giữa các phòng, đơn vị thuộc Sở Tư pháp và giữa các công chức, viên chức, người lao động trong cơ quan.

II. NỘI DUNG

1. Các quy định chung

a) Phạm vi điều chỉnh

Phương án ứng phó sự cố bảo đảm an toàn thông tin mạng quy định về việc phối hợp ứng phó sự cố an toàn thông tin mạng (ATTT) trong hoạt động ứng dụng công nghệ thông tin, chuyển đổi số của Sở Tư pháp tỉnh Tuyên Quang.

b) Đối tượng áp dụng

- Các phòng, đơn vị thuộc Sở, các đơn vị sự nghiệp trực thuộc Sở.

- Cá nhân là công chức, viên chức và người lao động của cơ quan, đơn vị thuộc, trực thuộc Sở và các tổ chức, cá nhân khác liên quan.

c) Nguyên tắc, phương châm ứng phó sự cố

Sự cố ATTT mạng, hệ thống thông tin cần ứng phó khi bị một trong các sự cố sau:

- Hệ thống bị gián đoạn dịch vụ.

- Dữ liệu tuyệt mật hoặc bí mật nhà nước có khả năng bị tiết lộ.

- Dữ liệu quan trọng của hệ thống không đảm bảo tính toàn vẹn và không có khả năng khôi phục được.

- Hệ thống bị mất quyền điều khiển.

- Sự cố có khả năng xảy ra trên diện rộng hoặc gây ra các ảnh hưởng dây chuyền.

- Chủ quản hệ thống thông tin không đủ khả năng kiểm soát, xử lý được sự cố.

d) Chức năng, nhiệm vụ, trách nhiệm và cơ chế, quy trình phối hợp giữa các lực lượng tham gia ứng cứu sự cố.

- Phòng Xây dựng, kiểm tra, thi hành pháp luật và phổ biến, giáo dục pháp luật là bộ phận đầu mối, chủ trì ứng cứu sự cố ATTT mạng của Sở có trách nhiệm tham gia hoạt động ứng cứu khẩn cấp đảm bảo ATTT mạng nội bộ khi có yêu cầu từ các phòng, đơn vị thuộc Sở.

- Các phòng, đơn vị thuộc Sở có trách nhiệm phối hợp ứng cứu sự cố ATTT khi xảy ra sự cố.

2) Đánh giá các nguy cơ, sự cố an toàn thông tin mạng

a) Đánh giá hiện trạng và khả năng đảm bảo ATTT mạng của các hệ thống thông tin và các đối tượng cần bảo vệ.

b) Đánh giá, dự báo nguy cơ, sự cố, tấn công mạng có thể xảy ra với các hệ thống thông tin và các đối tượng cần bảo vệ.

c) Đánh giá, dự báo các hậu quả, thiệt hại, tác động có thể có nếu xả ra sự cố.

d) 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 *(bao gồm cả nhà thầu đã ký hợp đồng cung cấp dịch vụ nếu có)*.

- *Đơn vị chủ trì:* Các phòng, đơn vị thuộc Sở, các đơn vị sự nghiệp trực thuộc Sở.

- *Đơn vị phối hợp:* Phòng Xây dựng, kiểm tra, thi hành pháp luật và phổ biến, giáo dục pháp luật; Đội ứng cứu sự cố mạng, máy tính tỉnh Tuyên Quang; Đơn vị cung cấp dich vụ ATTT mạng.

- *Thời gian thực hiện:* Thường xuyên.

3. Phương án đối phó, ứng cứu sự cố đối với một số tình huống sự cố cụ thể

Phương án đối phó, ứng cứu sự cố ATTT mạng phải đặt ra 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. Việc xây dựng phương án đối phó, ứng cứu sự cố ATTT mạng cần đảm bảo các nội dung sau:

a) Phương pháp, cách thức để xác định nhanh chóng, 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 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…

b) 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 mạng 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, …

c) Công tác tổ chức, điều hành, phối hợp giữa các lực lượng, giữa các tổ chức trong đối phó, ngăn chặn, ứng cứu, khắc phục sự cố.

- *Đơn vị chủ trì:* Các phòng, đơn vị thuộc Sở, các đơn vị sự nghiệp trực thuộc Sở.

- *Đơn vị phối hợp:* Phòng Xây dựng, kiểm tra, thi hành pháp luật và phổ biến, giáo dục pháp luật; Đội ứng cứu sự cố mạng, máy tính tỉnh Tuyên Quang; Đơn vị cung cấp dich vụ ATTT mạng.

- *Thời gian thực hiện:* Hàng năm

4. Triển khai phòng ngừa sự cố, giám sát phát hiện, đảm bảo các điều kiện sẵn sàng ứng phó, khắc phục sự cố

a) Các nội dung, nhiệm vụ cụ thể cần triển khai nhằm phòng ngừa sự cố, đảm bảo các điều kiện sẵn sàng ứng phó, khắc phục sự cố

- Các nội dung nhằm phát hiện sớm và phòng ngừa sự cố

- Thực hiện nghiêm công tác giám sát, phát hiện sớm nguy cơ sụp đổ.

- Kiểm tra, đánh giá ATTT 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 ATTT mạng, phần mềm độc hại.

- Xây dựng, áp dụng quy trình, quy định, tiêu chuẩn về ATTT; tuyên truyền, nâng cao nhận thức về nguy cơ, sự cố tấn công mạng.

b) Các nội dung nhằm đảm bảo các điều kiện sẵn sàng ứng phó, khắc phục sự cố.

- Trang bị, nâng cấp thiết bị, công cụ, phương tiện, gia hạn bản quyền phần mềm phục vụ việc ứng cứu, khắc phục sự cố.

- Thuê dịch vụ đảm bảo ATTT, chuẩn bị các nguồn lực sẵn sàng để ứng phó, khắc phục khi sự cố xả ra.

- Tham gia các lớp tập huấn, các hoạt động của mạng lưới ứng cứu sự cố.

+ Đơn vị chủ trì: Phòng Xây dựng, kiểm tra, thi hành pháp luật và phổ biến, giáo dục pháp luật; Các phòng, đơn vị thuộc Sở, các đơn vị sự nghiệp trực thuộc Sở.

+ Đơn vị phối hợp: Đội ứng cứu sự cố mạng, máy tính tỉnh Tuyên Quang; Đơn vị cung cấp dich vụ ATTT mạng.

+ Thời gian thực hiện: Hàng năm.

5. Tổ chức thực hiện

- Phòng Xây dựng, kiểm tra, thi hành pháp luật và phổ biến, giáo dục pháp luật: chủ trì, phối hợp với các phòng, đơn vị thuộc Sở, các đơn vị sự nghiệp trực thuộc Sở triển khai thực hiện các nội dung của kế hoạch này; tiến hành kiểm tra công tác đảm bảo ATTT mạng định kỳ hàng quý hoặc theo hướng dẫn của cơ quan chuyên môn. Là đầu mối tiếp nhận các sự cố về ATTT mạng trong hoạt động của cơ quan. Triển khai điều hành, phối hợp tổ chức ứng cứu và thực hiện ứng cứu, xử lý, ngăn chặn, khắc phục sự cố ATTT mạng.

- Văn phòng Sở: Tham mưu Giám đốc Sở bảo đảm kinh phí triển khai thực hiện các nội dung của kế hoạch này.

- Các phòng, đơn vị thuộc Sở, các đơn vị sự nghiệp trực thuộc Sở: Chủ động thông báo với Phòng Xây dựng, kiểm tra, thi hành pháp luật và phổ biến, giáo dục pháp luật khi phát hiện ra sự số liên quan đến ATTT mạng đồng thời phối hợp với Phòng Xây dựng, kiểm tra, thi hành pháp luật và các đơn vị liên quan thực hiện công tác ứng phó sự cố ATTT mạng tại đơn vị mình.

Trên đây là Kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng của Sở Tư pháp tỉnh Tuyên Quang. Trong quá trình triển khai thực hiện, nếu có vấn đề phát sinh, vướng mắc, các phòng, đơn vị phản hồi về Phòng Xây dựng, kiểm tra, thi hành pháp luật và phổ biến, giáo dục pháp luật để tổng hợp, báo cáo lãnh đạo Sở xem xét, sửa đổi, bổ sung./.

Nơi nhận:
- UBND tỉnh (báo cáo);
- Sở TTTT;
- Giám đốc Sở;
- Các PGĐ Sở;
- Các phòng, đơn vị thuộc Sở,
Các đơn vị sự nghiệp trực thuộc Sở.
- Lưu: VT, XDKTTHPL&PBGDPL.(Đ. Thành)

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HOÀ X.H.C.N VIỆT NAM
SỞ TƯ PHÁP
TỈNH TUYÊN QUANG

Đặng Thị Thanh Hương