UBND TỈNH ĐẮK NÔNG **SỞ LAO ĐỘNG THƯƠNG BINH VÀ XÃ HỘI**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 971/KH-SLĐTBXH	*Đắk Nông, ngày 28 tháng 5 năm 2019*

KẾ HOẠCH
Ứng phó sự cố an toàn thông tin mạng năm 2019

Thực hiện Kế hoạch số 19/KH-ĐƯCSCATTTM ngày 28/3/2019 của Đội Ứng cứu sự cố an toàn thông tin mạng về Kế hoạch hoạt động của Đội Ứng cứu sự cố an toàn thông tin mạng tỉnh Đắk Nông năm 2019. Sở Lao động - Thương binh và Xã hội xây dựng Kế hoạch Ứng phó sự cố an toàn thông tin mạng năm 2019 với những nội dung cụ thể như sau:

I. CĂN CỨ LẬP KẾ HOẠCH

Căn cứ Luật Công nghệ thông tin ngày 29/6/2006;

Căn cứ Luật An toàn thông tin mạng ngày 19/11/2015;

Căn cứ 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 898/QĐ-TTg ngày 27/5/2016 của Thủ tướng Chính phủ phê duyệt phương hướng, mục tiêu, nhiệm vụ bảo đảm an toàn thông tin mạng giai đoạn 2016 - 2020;

Căn cứ 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;

Căn cứ 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 ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ 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;

Căn cứ Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin;

Căn cứ Quyết định số 1304/QĐ-UBND ngày 15/8/2017 của Ủy ban nhân dân tỉnh Đắk Nông về việc thành lập Đội Ứng cứu sự cố an toàn thông tin mạng tỉnh Đắk Nông;

Căn cứ Quyết định số 25/QĐ-ĐỨCCATTTM ngày 10/5/2018 của Đội trưởng Đội Ứng cứu sự cố an toàn thông tin mạng tỉnh Đắk Nông về việc ban hành "Quy chế hoạt động của Đội Ứng cứu sự cố an toàn thông tin mạng tỉnh Đắk Nông".

II. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Bảo đảm an toàn thông tin mạng (sau đây viết tắt là ATTTM) của đơn vị, trong đó tập trung an toàn thông tin cho các hệ thống thông tin quan trọng, có khả năng thích ứng một cách chủ động, linh hoạt và giảm thiểu các nguy cơ, đe dọa mất ATTTM. Đề ra các giải pháp ứng phó khi gặp sự cố mất ATTTM.

- Tạo chuyển biến mạnh mẽ trong nhận thức về an toàn thông tin đối với lực lượng cán bộ, công chức, viên chức, người lao động.

- Nâng cao năng lực, hiệu quả hoạt động mạng lưới ứng cứu sự cố ATTTM của đơn vị, gắn kết với các đơn vị thành viên, hợp tác, kết nối chặt chẽ, điều phối kịp thời, phối hợp đồng bộ, hiệu quả của các lực lượng để ứng cứu sự cố mạng, chống tấn công mạng.

- Bảo đảm 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 ATTTM.

2. Yêu cầu

- Phải khảo sát, đánh giá các nguy cơ, sự cố ATTTM của hệ thống thông tin để đưa ra phương án đối phó, ứng cứu sự cố phù hợp, kịp thời.

- Phương án đối phó, ứng cứu sự cố ATTTM 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.

- Ứng cứu sự cố trước hết phải được thực hiện, xử lý bằng lực lượng tại chỗ và trách nhiệm chính của chính đơn vị.

- Thông tin trao đổi trong mạng lưới phải được kiểm tra, xác thực đối tượng trước khi thực hiện các bước tác nghiệp tiếp theo.

- Bảo đảm bí mật thông tin biết được khi tham gia, thực hiện các hoạt động ứng cứu sự cố theo yêu cầu của Cơ quan điều phối quốc gia hoặc cơ quan tổ chức, cá nhân gặp sự cố.

- Chủ động liên hệ với Đội Ứng cứu sự cố ATTTM tỉnh Đắk Nông khi có nhu cầu cần hỗ trợ ứng cứu hệ thống khi gặp sự cố mà đơn vị không tự khắc phục được.

- Nguồn lực đảm bảo, giải pháp tổ chức thực hiện và kinh phí để triển khai các nội dung của Kế hoạch, đảm bảo khả thi, hiệu quả.

III. NỘI DUNG

1. Tuyên truyền, phổ biến các văn bản quy phạm pháp luật; hướng dẫn nâng cao nhận thức, kiến thức, kỹ năng về ATTTM

- Tuyên truyền, phổ biến về 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 898/QĐ-TTg ngày 27/5/2016 của Thủ tướng Chính phủ phê duyệt phương hướng, mục tiêu, nhiệm vụ bảo đảm ATTTM giai đoạn 2016 - 2020; 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 ATTTM 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 ATTTM trên toàn quốc.

- Hướng dẫn nâng cao nhận thức, kiến thức, kỹ năng về ATTTM cho cán bộ, công chức, viên chức, người lao động.

- Thực hiện: Văn phòng Sở; các phòng chuyên môn, đơn vị trực thuộc Sở.

- Thời gian thực hiện: hướng dẫn thông qua các văn bản hàng năm.

2. Đánh giá các nguy cơ, sự cố ATTTM

Đánh giá hiện trạng và khả năng bảo đảm ATTTM của các hệ thống thông tin và các đối tượng cần bảo vệ; đánh giá, dự báo các nguy cơ, sự cố, tấn công mạng có thể xảy ra với các hệ thống thông tin và các đối tượng cần bảo vệ; 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 (bao gồm của cả nhà thầu đã ký hợp đồng cung cấp dịch vụ nếu có).

- Đơn vị thực hiện: Văn phòng Sở.

- Đơn vị phối hợp: Sở Thông tin và Truyền thông; Đội Ứng cứu sự cố ATTTM tỉnh Đắk Nông; Nhà thầu cung cấp dịch vụ an toàn thông tin mạng (nếu có); các đơn vị liên quan khác.

- Thời gian thực hiện: Thường xuyên trong năm hoặc đột xuất.

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

Đối với mỗi hệ thống thông tin cần xây dựng tình huống, kịch bản sự cố cụ thể và đưa ra phương án đối phó, ứng cứu sự cố tương ứng. 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. Việc xây dựng phương án đối phó, ứng cứu sự cố 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 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...

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 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....

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

* Văn phòng Sở có trách nhiệm:

- Hướng dẫn công tác điều phối, ứng cứu sự cố ATTTM đến các phòng chuyên môn, đơn vị trực thuộc Sở, tuân thủ yêu cầu của Đội Ứng cứu sự cố ATTTM tỉnh Đắk Nông, Cơ quan điều phối quốc gia trong điều phối, ứng cứu sự cố.

* Các phòng chuyên môn, đơn vị trực thuộc có trách nhiệm như sau:

- Chủ động thực hiện Kế hoạch, chủ động giám sát theo quy định hiện hành.

- Khảo sát, kiểm tra, đánh giá an toàn thông tin cho các hệ thống thông tin quan trọng hoặc có nguy cơ bị tấn công cao.

- Xây dựng và triển khai các phương án khắc phục điểm yếu (nếu có), bảo vệ hoặc phòng ngừa để giảm thiểu thiệt hại khi có tấn công, sự cố ATTTM.

- Triển khai các biện pháp sao lưu dự phòng để nâng cao khả năng phục hồi hệ thống khi xảy ra sự cố.

4. Báo cáo sự cố ATTTM

- Đơn vị thực hiện: Văn phòng Sở; các phòng chuyên môn, đơn vị trực thuộc Sở.

- Đơn vị phối hợp: Sở Thông tin và Truyền thông, Đội Ứng cứu sự cố ATTTM tỉnh Đắk Nông.

- Thời gian thực hiện: Ngay khi xảy ra sự cố và được duy trì trong suốt quá trình ứng cứu sự cố.

5. Tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố ATTTM

- Đơn vị chủ trì: Văn phòng Sở.

- Đơn vị phối hợp: Sở Thông tin và Truyền thông, Đội Ứng cứu sự cố ATTTM tỉnh Đắk Nông.

- Thời gian thực hiện: Ngay sau khi phát hiện sự cố hoặc nhận được thông báo, báo cáo sự cố.

6. Quy trình ứng cứu sự cố ATTTM

- Đơn vị chủ trì: Văn phòng Sở.

- Đơn vị phối hợp: Sở Thông tin và Truyền thông, Đội Ứng cứu sự cố ATTTM tỉnh Đắk Nông.

- Thời gian thực hiện: Ngay khi xảy ra sự cố và được duy trì trong suốt quá trình ứng cứu sự cố.

IV. TỔ CHỨC THỰC HIỆN

1. Các phòng chuyên môn, đơn vị trực thuộc Sở

- Căn cứ vào nội dung Kế hoạch triển khai thực hiện.

- Nâng cao nhận thức, trách nhiệm của từng cá nhân trong quá trình sử dụng hệ thống mạng của đơn vị.

2. Văn phòng Sở

- Là cơ quan thường trực triển khai thực hiện Kế hoạch này.

- Theo dõi, đôn đốc, kiểm tra, giám sát công tác bảo đảm ATTTM đối với các phòng chuyên môn.

3. Phòng Kế hoạch - Tài chính

- Cần bảo vệ dự toán hàng năm và từng giai đoạn đối với Sở Tài chính để bố trí ngân sách cho đơn vị đảm bảo kinh phí thực hiện.

- Kết hợp kinh phí được cấp từ nguồn ngân sách trung ương, ngân sách địa phương và các nguồn kinh phí hợp pháp khác để triển khai Kế hoạch.

- Sử dụng ngân sách phù hợp để thực hiện các nội dung như: đào tạo về kiến thức ATTTM cho các cán bộ, công chức, viên chức, người lao động, nâng cao năng lực, nhận thức; mua sắm các trang thiết bị cần thiết cho nhu cầu triển khai Kế hoạch.

- Căn cứ các nhiệm vụ trong Kế hoạch để thẩm định, tham mưu bố trí ngân sách nhà nước hàng năm của đơn vị triển khai Kế hoạch này.

Văn phòng Sở yêu cầu lãnh đạo các phòng chuyên môn, đơn vị trực thuộc nghiêm túc triển khai thực hiện Kế hoạch này. Trong quá trình triển khai thực hiện

Kế hoạch, nếu có vướng mắc, vui lòng liên hệ về Văn phòng Sở để tổng hợp, báo cáo cơ quan có thẩm quyền xem xét, quyết định./.

Nơi nhận:
- Sở TT&TT (b/c);
- Đội UCSCATTTM (b/c);
- Ban Giám đốc Sở;
- Các phòng chuyên môn, ĐVTT (th/hiện);
- Lưu: VT, VP.

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ LAO ĐỘNG THƯƠNG BINH VÀ XÃ HỘI
TỈNH ĐẮK NÔNG

Người ký: Sở Lao động - Thương binh và Xã hội
Email: sldtbxh@daknong.gov.vn
Cơ quan: Tỉnh Đắk Nông
Thời gian ký: 28.05.2019 14:23:45 +07:00

Huỳnh Ngọc Anh