

QUYẾT ĐỊNH

**Ban hành Kế hoạch ứng phó sự cố bảo đảm an toàn
thông tin mạng trên địa bàn tỉnh Đắk Nông**

ỦY BAN NHÂN DÂN TỈNH ĐẮK NÔNG

Căn cứ Luật Tổ chức Chính quyền địa phương ngày 19/6/2015;

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 25/7/2016 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 Quyết định số 1622/QĐ-TTg ngày 25/10/2017 của Thủ tướng Chính phủ phê duyệt đề án đẩy mạnh hoạt động của mạng lưới ứng cứu sự cố, tăng cường năng lực cho các cán bộ, bộ phận chuyên trách ứng cứu sự cố an toàn thông tin mạng trên toàn quốc đến 2020, định hướng đến 2025;

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 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 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;

Xét đề nghị của Sở Thông tin và Truyền thông tại Tờ trình số 57/TTr-STTTT ngày 04/12/2017,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Đắk Nông.

Điều 2. Quyết định này có hiệu lực kể từ ngày ký ban hành.



Trưởng Ban Chỉ đạo cải cách hành chính tỉnh; Chánh Văn phòng UBND tỉnh; Giám đốc các Sở: Thông tin và Truyền thông, Tài chính, Kế hoạch và Đầu tư; Chủ tịch UBND các huyện, thị xã và Thủ trưởng các Sở, Ban, ngành, cơ quan, đơn vị có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:

- Như Điều 2;
- Bộ TT&TT (b/c);
- Thường trực Tỉnh ủy (b/c);
- Thường trực HĐND tỉnh (b/c);
- CT, các PCT UBND tỉnh;
- Ban chỉ đạo CCHC tỉnh;
- Công TTĐT tỉnh;
- CVP, các PCVP UBND tỉnh;
- Lưu VT, CNXD, KGVX (Q).

5

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH



Tôn Thị Ngọc Hạnh

ỦY BAN NHÂN DÂN CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
TỈNH ĐẮK NÔNG **Độc lập - Tự do - Hạnh phúc**

Đắk Nông, ngày 19 tháng 12 năm 2017

KẾ HOẠCH

Ứng phó sự cố bảo đảm an toàn thông tin mạng
trên địa bàn tỉnh Đắk Nông

(Kèm theo Quyết định số 2005/QĐ-UBND ngày 19/12/2017 của UBND tỉnh)

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

a) Bảo đảm an toàn thông tin mạng của tỉnh, trong đó tập trung bảo đảm an toàn thông tin cho các hệ thống thông tin quan trọng của tỉnh, có khả năng thích ứng một cách chủ động, linh hoạt và giảm thiểu các nguy cơ, đe dọa mất an toàn thông tin trên mạng. Đề ra các giải pháp ứng phó khi gặp sự cố mất an toàn thông tin mạng.

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

c) 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 an toàn thông tin mạng.

2. Yêu cầu

a) Phải khảo sát, đánh giá các nguy cơ, sự cố an toàn thông tin mạng của toàn hệ thống để đưa ra phương án đối phó, ứng cứu sự cố tương ứng, kịp thời, phù hợp.

b) Phương án đối phó, ứng cứu sự cố an toàn thông tin mạng 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.

II. NHIỆM VỤ TRIỂN KHAI

1. Tuyên truyền, phổ biến các văn bản quy phạm pháp luật; Tập huấn nâng cao nhận thức, kiến thức, kỹ năng về an toàn thông tin mạng

- Tuyên truyền nâng cao nhận thức cho cán bộ, công chức, viên chức trên địa bàn tỉnh về ý nghĩa và tầm quan trọng của việc bảo đảm an toàn an ninh thông tin tại mỗi cơ quan đơn vị. Tối thiểu phải hiểu: An toàn thông tin là sự bảo vệ thông tin và hệ thống thông tin tránh bị truy cập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin. Trong đó hệ thống thông tin là tập hợp các thiết bị phần cứng, phần mềm và cơ sở dữ liệu phục vụ mục đích thu thập, xử lý, lưu trữ, trao đổi thông tin; Nguy cơ mất an toàn thông tin là những nhân tố bên trong hoặc bên ngoài hệ thống thông tin có khả năng ảnh hưởng tới trạng thái an toàn thông tin; Bảo đảm an toàn thông tin bao gồm các hoạt động nhằm bảo vệ tính bảo mật, tính toàn vẹn, tính sẵn sàng của thông tin.

- Tổ chức hội nghị 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 25/7/2016 của Thủ tướng Chính phủ phê duyệt phương hướng, mục tiêu, nhiệm vụ bảo đảm an toàn thông tin mạng giai đoạn 2016-2020; 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; 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 số 85/2016/NĐ-CP.

- Đơn vị chủ trì: Sở Thông tin và Truyền thông.

- Đơn vị phối hợp: Các Sở, ngành; UBND cấp huyện; các đơn vị có liên quan của tỉnh.

- Thời gian thực hiện: Trong năm 2018 và những năm tiếp theo.

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

Đánh giá hiện trạng và khả năng bảo đảm an toàn thông tin mạng 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.

- Đơn vị thực hiện: Các Sở, ngành; UBND cấp huyện.

- Đơn vị phối hợp: Đơn vị chuyên trách ứng cứu sự cố (Sở Thông tin và Truyền thông); Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh; Đơn vị 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.

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

Đối với mỗi hệ thống thông tin, chương trình, ứng dụng, 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 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 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 dữ liệu, phần mềm, 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

Thực hiện theo quy định tại 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 và Quy chế hoạt động Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Đắk Nông.

- Đơn vị phối hợp: Cơ quan điều phối quốc gia (Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam - VNCERT); Ban Chỉ đạo Cải cách hành chính tỉnh; tổ chức, cá nhân gửi thông báo, báo cáo sự cố; đơn vị cung cấp dịch vụ an toàn thông tin mạng (nếu có); các đơn vị chức năng liên quan.

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

c) Quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13 và Điều 14 Quyết định số 05/2017/QĐ-TTg

Đơn vị vận hành các hệ thống thông tin (các Sở, ngành; UBND cấp huyện); Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Đắk Nông khi được giao nhiệm vụ xử lý sự cố an toàn thông tin mạng từ cơ quan điều phối phải tuân thủ quy trình được quy định tại Điều 13 và Điều 14 Quyết định số 05/2017/QĐ-TTg.

5. Triển khai huấn luyện, diễn tập, phòng ngừa sự cố, giám sát phát hiện, bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố

Xây dựng các nội dung, nhiệm vụ cụ thể cần triển khai nhằm phòng ngừa sự cố, giám sát phát hiện, huấn luyện, diễn tập, bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố, cụ thể bao gồm:

a) Triển khai các chương trình huấn luyện, diễn tập:

- Huấn luyện, diễn tập các phương án đối phó, ứng cứu sự cố tương ứng với các kịch bản, tình huống sự cố cụ thể; Huấn luyện, diễn tập nâng cao kỹ năng, nghiệp vụ phối hợp, ứng cứu, chống tấn công, xử lý mã độc, khắc phục sự cố; tham gia huấn luyện, diễn tập vùng, miền, quốc gia, quốc tế.

- Đơn vị chủ trì: Sở Thông tin và Truyền thông, Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Đắk Nông.

- Đơn vị phối hợp: Đơn vị vận hành các hệ thống thông tin (các Sở, ngành; UBND cấp huyện); Cơ quan điều phối quốc gia (Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam - VNCERT); các đơn vị chức năng liên quan.

- Thời gian thực hiện: Hàng năm.

b) Các nội dung, nhiệm vụ nhằm phòng ngừa sự cố và phát hiện sớm sự cố:

- Giám sát, phát hiện sớm nguy cơ, sự cố; kiểm tra, đánh giá an toàn thông tin 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 an toàn thông tin mạng, phần mềm độc hại; xây dựng, áp dụng quy trình, quy định, tiêu chuẩn an toàn thông tin; Tuyên truyền, nâng cao nhận thức về nguy cơ, sự cố, tấn công mạng.

- Đơn vị chủ trì: Sở Thông tin và Truyền thông, Đơn vị vận hành các hệ thống thông tin (các Sở, ngành; UBND cấp huyện); Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Đắk Nông.

d) *Phương án về nhân lực, trang thiết bị, phần mềm, phương tiện, công cụ và dự kiến kinh phí để thực hiện, đối phó, ứng cứu, xử lý đối với từng tình huống sự cố cụ thể:*

- Đơn vị chủ trì: Các Sở, ngành; UBND cấp huyện.

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

- Thời gian thực hiện: Hàng năm.

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

Triển khai các hoạt động thuộc trách nhiệm của các cơ quan, đơn vị liên quan theo quy định tại các Điều 11, Điều 12, Điều 13, Điều 14 và các nội dung liên quan khác của 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 (*sau đây gọi tắt là Quyết định số 05/2017/QĐ-TTg*).

Dự phòng kinh phí, nhân lực, vật lực thường trực sẵn sàng ứng cứu sự cố; triển khai điều hành phối hợp tổ chức ứng cứu và thực hiện ứng cứu, xử lý, ngăn chặn, khắc phục sự cố khi có sự cố xảy ra.

a) *Báo cáo sự cố an toàn thông tin mạng theo quy định tại Điều 11 Quyết định số 05/2017/QĐ-TTg*

- Đơn vị thực hiện:

+ Đơn vị vận hành các hệ thống thông tin (các Sở, ngành; UBND cấp huyện) báo cáo cơ quan Chủ quản hệ thống thông tin, Sở Thông tin và Truyền thông, đồng gửi cơ quan điều phối quốc gia (Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam - VNCERT, địa chỉ: 115 Trần Duy Hưng, Trung Hòa, Cầu Giấy, Hà Nội, Website: www.vncert.gov.vn);

+ Sở Thông tin và Truyền thông báo cáo Cơ quan chủ quản hệ thống thông tin, Ban Chỉ đạo ứng dụng công nghệ thông tin tỉnh (nay được sáp nhập vào Ban Chỉ đạo cải cách hành chính tỉnh) và Cơ quan điều phối quốc gia;

+ Ban Chỉ đạo ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh (tỉnh không thành lập Ban chỉ đạo mà bổ sung chức năng nhiệm vụ vào Ban Chỉ đạo cải cách hành chính tỉnh) thực hiện báo cáo Cơ quan thường trực và Ban Chỉ đạo quốc gia về ứng cứu sự cố.

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

b) *Tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng theo quy định tại Điều 12 Quyết định số 05/2017/QĐ-TTg*

- Đơn vị chủ trì: Sở Thông tin và Truyền thông, Đơn vị vận hành các hệ thống thông tin (các Sở, ngành; UBND cấp huyện); Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Đắk Nông.

- Đơn vị phối hợp: Cơ quan điều phối quốc gia (Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam - VNCERT); các đơn vị chức năng liên quan.

- Thời gian thực hiện: Thường xuyên trong năm.

c) Các nội dung, nhiệm vụ nhằm bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố

Trang bị, nâng cấp trang thiết bị, công cụ, phương tiện, gia hạn bản quyền phục vụ ứng cứu, khắc phục sự cố; chuẩn bị các điều kiện bảo đảm, dự phòng các nguồn lực và tài chính để sẵn sàng đối phó, ứng cứu, khắc phục khi sự cố xảy ra; tổ chức hoạt động của đội ứng cứu sự cố; thuê dịch vụ kỹ thuật và tổ chức, duy trì đội chuyên gia ứng cứu sự cố; tổ chức và tham gia các hoạt động của mạng lưới ứng cứu sự cố.

- Đơn vị chủ trì: Sở Thông tin và Truyền thông, Đơn vị vận hành các hệ thống thông tin (các Sở, ngành; UBND cấp huyện); Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Đắk Nông.

- Đơn vị phối hợp: Cơ quan điều phối quốc gia (Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam - VNCERT); các đơn vị chức năng liên quan.

- Thời gian thực hiện: Hàng năm.

6. Các giải pháp đảm bảo triển khai kế hoạch

a) Chỉ đạo, điều hành

Ban Chỉ đạo ứng dụng công nghệ thông tin tỉnh (Ban chỉ đạo Cải cách hành chính tỉnh) tăng cường chỉ đạo về an toàn thông tin số trong hoạt động của cơ quan nhà nước.

Tiếp tục hoàn thiện bộ máy quản lý nhà nước về an toàn thông tin số từ UBND tỉnh đến các Sở, Ban, ngành, huyện, thị xã; trong đó chú trọng nâng cao năng lực của các cán bộ chuyên trách về an toàn thông tin số (Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Đắk Nông).

b) Giải pháp tài chính

Tập trung đầu tư các dự án, nhiệm vụ độc lập về an toàn thông tin số sử dụng nguồn vốn đầu tư từ nguồn vốn triển khai Dự án Chính quyền điện tử tỉnh Đắk Nông nhằm đạt được các chỉ tiêu đã đề ra, tạo cơ sở pháp lý và nền tảng hạ tầng cho các giai đoạn sau này.

Các Sở, Ban, ngành và các UBND huyện, thị xã: Trên cơ sở kế hoạch của từng đơn vị trong kế hoạch ngân sách hàng năm, phải có mục chi cho công nghệ thông tin về bảo đảm an toàn thông tin số để thực hiện các dự án công nghệ thông tin thuộc phạm vi của đơn vị; tự bảo đảm an toàn thông tin số tại đơn vị mình.

c) Giải pháp kỹ thuật đảm bảo an toàn, an ninh thông tin:

Quan tâm đầu tư trang bị thiết bị về an toàn thông tin; xem đầu tư hạng mục an toàn, an ninh thông tin là khoản đầu tư thiết yếu; có kế hoạch mua sắm,

trang bị phần mềm diệt virus có bản quyền; các thiết bị chuyên dụng cho an toàn và bảo mật thông tin; thực hiện bảo trì, bảo dưỡng định kỳ các thiết bị an toàn, bảo mật thông tin.

Tăng cường ký số các loại văn bản điện tử theo quy định nhằm đảm bảo an toàn trong việc trao đổi văn bản điện tử qua môi trường mạng; hệ thống xác thực tài khoản và mã hóa dữ liệu...

Tăng cường sử dụng thư điện tử công vụ để gửi các văn bản, trao đổi công việc trong các cơ quan nhà nước, tuyệt đối không sử dụng các hộp thư điện tử miễn phí (Gmail, Yahoo...) nhằm bảo đảm bảo mật, an toàn thông tin trên môi trường mạng.

Thường xuyên cập nhật các bản vá cập nhật phần mềm từ các nhà cung cấp sản phẩm, dịch vụ. Ngoài ra, với các tài khoản email, facebook..., cần thay đổi mật khẩu theo định kỳ, hạn chế việc sử dụng email miễn phí, trong trường hợp có đính kèm các tài liệu quan trọng gửi qua email phải đặt mật khẩu để bảo đảm an toàn...

Triển khai giải pháp lưu nhật ký đối với các hệ thống thông tin quan trọng; Đầu tư, trang bị các hệ thống giám sát mạng và cảnh báo sớm các dấu hiệu tấn công mạng. Thiết lập hệ thống sao lưu dự phòng, bảo đảm tránh rủi ro mất dữ liệu khi có sự cố xảy ra.

d) Giải pháp kiểm tra, giám sát:

Thường xuyên rà soát tiến độ triển khai kế hoạch bảo đảm an toàn thông tin số tại các cơ quan nhà nước của tỉnh.

Tăng cường công tác kiểm tra định kỳ về an toàn thông tin số.

Tổ chức đánh giá định kỳ và công bố các báo cáo hàng năm về năng lực đảm bảo an toàn thông tin số đối với các hệ thống thông tin quan trọng của tỉnh.

đ) Giải pháp môi trường chính sách

Rà soát và hoàn thiện các văn bản quy phạm pháp luật, cơ chế và chính sách của tỉnh, tạo môi trường thuận lợi để bảo đảm an toàn thông tin số, đáp ứng các yêu cầu về hội nhập toàn diện kinh tế quốc tế, thúc đẩy hợp tác với các doanh nghiệp, tổ chức trong và ngoài nước trong lĩnh vực an toàn thông tin số. Xây dựng các tiêu chuẩn, quy chuẩn kỹ thuật, xác định chiến lược, quy hoạch chính sách an toàn thông tin của tỉnh. Tại các cơ quan, đơn vị ban hành đầy đủ các quy định nội bộ về công tác bảo đảm an toàn an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin phù hợp với tình hình, an ninh mạng trong tình hình mới.

Xây dựng quy chế an toàn thông tin số chung cho các cơ quan nhà nước của tỉnh: Nghiên cứu và ban hành các quy định về quy chế, chính sách thực hiện bảo đảm an toàn, an ninh thông tin tuân thủ theo tiêu chuẩn ISO 27001 và tiêu chuẩn ISO 19001.

Xây dựng quy trình và các hướng dẫn thực hiện bảo đảm an toàn thông tin số trong nội bộ cơ quan nhà nước của tỉnh: Nghiên cứu các quy trình bảo mật và đảm bảo an toàn thông tin cho cán bộ quản trị hệ thống, nhân viên kiểm soát an ninh và người sử dụng hệ thống khi giao tiếp, trao đổi; ban hành các quy chuẩn về hệ thống máy tính, trang thiết bị, máy chủ, phần mềm hệ thống, phần mềm nghiệp vụ...

Xây dựng tài liệu chỉ dẫn an toàn thông tin số, chỉ dẫn phát triển ứng dụng bảo đảm an toàn thông tin số cho các đối tượng người sử dụng, công dân và các doanh nghiệp phát triển phần mềm.

e) Nâng cao nhận thức

Tăng cường công tác tuyên truyền, phổ biến: Tổ chức tuyên truyền để cán bộ, đảng viên và nhân dân nhận thức đầy đủ vị trí, vai trò và tầm quan trọng của công tác bảo đảm an toàn thông tin mạng, tuyên truyền rộng rãi nhằm nâng cao nhận thức của người dân, doanh nghiệp về lợi ích ứng dụng công nghệ thông tin và tầm quan trọng của việc bảo đảm an toàn thông tin.

Đặc biệt chú trọng nâng cao nhận thức của người dân trong việc bảo đảm an toàn thông tin trong khai thác sử dụng Internet, trong các giao dịch dịch vụ công trực tuyến với các cơ quan Nhà nước, trong các giao dịch điện tử... để tránh thành nạn nhân mạng cũng như vô tình tiếp tay cho các hoạt động phi pháp của tội phạm mạng.

Tăng cường hợp tác để học tập kinh nghiệm trong nước và quốc tế trong việc bảo đảm an toàn thông tin số.

III. KINH PHÍ

1. Kinh phí thực hiện

Kinh phí thực hiện Kế hoạch được bố trí từ nguồn ngân sách hàng năm của tỉnh. Bên cạnh đó cần huy động từ các nguồn sau:

- Nguồn vốn hỗ trợ từ ngân sách Trung ương qua các chương trình, dự án triển khai theo ngành dọc từ Trung ương đến các địa phương; các chương trình mục tiêu quốc gia và các chương trình, dự án khác;

- Huy động nguồn vốn từ các doanh nghiệp, thuê dịch vụ của doanh nghiệp, các nhà tài trợ, các tổ chức trong và ngoài nước có nguyện vọng đầu tư, hỗ trợ cho lĩnh vực công nghệ thông tin của tỉnh.

2. Dự toán kinh phí hoạt động cho cơ quan thường trực Sở Thông tin và Truyền thông và Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Đắk Nông

Hàng năm, Sở Thông tin và Truyền thông lập dự toán kinh phí chi cho hoạt động của cơ quan thường trực và Đội ứng cứu sự cố an toàn thông tin mạng tỉnh và đưa vào Kế hoạch ứng dụng công nghệ thông tin trong hoạt động các cơ quan nhà nước trên địa tỉnh để triển khai thực hiện.

IV. TỔ CHỨC THỰC HIỆN

1. Các Sở, Ban, ngành; UBND các huyện, thị xã

- Xây dựng nội dung, lập dự toán kinh phí lồng ghép trong Kế hoạch ứng dụng công nghệ thông tin hàng năm của cơ quan, đơn vị mình để triển khai thực hiện các nhiệm vụ được giao tại Kế hoạch này.

- Phân công lãnh đạo phụ trách và thành lập hoặc chỉ định bộ phận đầu mối chịu trách nhiệm về an toàn thông tin mạng của cơ quan, đơn vị.

- Quan tâm, chú trọng đến công tác bảo đảm an toàn thông tin của đơn vị; Chủ động sử dụng kinh phí chi thường xuyên được giao hàng năm để trang bị phần mềm chống virus, thiết bị tường lửa cho hệ thống mạng máy tính, hệ thống thông tin tại đơn vị mình.

- Thực hiện xác định cấp độ, lập hồ sơ đề xuất cấp độ an toàn hệ thống thông tin theo quy định tại Điều 14 và Điều 15 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 và theo hướng dẫn tại 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 số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

- Phối hợp với Sở Thông tin và Truyền thông và các đơn vị liên quan thực hiện công tác ứng phó sự cố an toàn thông tin mạng trên địa bàn tỉnh.

- Định kỳ hàng năm, gửi báo cáo tình hình, kết quả về Sở Thông tin và Truyền thông để tổng hợp báo cáo UBND tỉnh hoặc báo cáo đột xuất khi cấp trên có yêu cầu.

2. Sở Thông tin và Truyền thông

- Là thành viên Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia; làm đầu mối, tổ chức hoạt động ứng cứu sự cố, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng trên địa bàn tỉnh, bộ phận trực tiếp tham mưu cho Sở Thông tin và Truyền thông xử lý sự cố là Đội ứng cứu sự cố an toàn thông tin mạng tỉnh; tham gia hoạt động ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia khi có yêu cầu từ Cơ quan thường trực hoặc Cơ quan điều phối.

- Tham mưu UBND tỉnh ban hành Kế hoạch triển khai Đề án đẩy mạnh hoạt động của mạng lưới ứng cứu sự cố, tăng cường năng lực cho các cán bộ, bộ phận chuyên trách ứng cứu sự cố an toàn thông tin mạng trên toàn quốc đến 2020, định hướng đến 2025 trên địa bàn tỉnh Đắk Nông.

- Tham mưu tổ chức thực thi, đôn đốc, kiểm tra, đánh giá, giám sát công tác bảo đảm an toàn thông tin định kỳ hàng năm hoặc theo chỉ đạo của UBND tỉnh đối với các cơ quan nhà nước trong tỉnh.

- Thẩm định, phê duyệt hoặc cho ý kiến về mặt chuyên môn đối với hồ sơ đề xuất cấp độ an toàn hệ thống thông tin theo thẩm quyền quy định tại Khoản 1,

Khoản 2 Điều 12 và Khoản 5 Điều 15 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 và theo hướng dẫn tại 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 số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

- Theo dõi, hướng dẫn, kiểm tra, giám sát việc thực hiện ứng phó sự cố đảm bảo an toàn thông tin mạng ở các Sở, Ban, ngành, UBND các huyện, thị xã.

- Xây dựng nội dung, lập dự toán kinh phí lồng ghép trong Kế hoạch ứng dụng công nghệ thông tin hàng năm của tỉnh để đảm bảo cho hoạt động của Đơn vị chuyên trách ứng cứu sự cố (Sở Thông tin và Truyền thông), Đội ứng cứu sự cố an toàn thông tin mạng tỉnh.

- Lập Báo cáo sơ kết 6 tháng triển khai Quyết định số 05/2017/QĐ-TTg (trước ngày 20/6) và Báo cáo tổng kết hàng năm thực hiện Quyết định số 05/2017/QĐ-TTg (trước ngày 20/12), gửi Bộ Thông tin và Truyền thông. Đồng thời, thực hiện báo cáo đột xuất khi cấp trên có yêu cầu.

3. Sở Kế hoạch và Đầu tư, Sở Tài chính

Căn cứ các nhiệm vụ trong Kế hoạch để thẩm định, tham mưu bố trí ngân sách nhà nước hàng năm của tỉnh cho các cơ quan, đơn vị, bảo đảm triển khai thực hiện tốt Kế hoạch này.

4. Trong quá trình thực hiện Kế hoạch này nếu có vấn đề vướng mắc, phát sinh, các cơ quan, đơn vị phản ánh kịp thời về Sở Thông tin và Truyền thông để tổng hợp báo cáo Ủy ban nhân dân tỉnh điều chỉnh, bổ sung./.

**TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH**



Tôn Thị Ngọc Hạnh