ỦY BAN NHÂN DÂN TỈNH GIA LAI	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 2050/KH-UBND	*Gia Lai, ngày 14 tháng 9 năm 2018*

KẾ HOẠCH
Ứng phó sự cố bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Gia Lai

I. CĂN CỨ LẬP KẾ HOẠCH:

Luật Công nghệ thông tin năm 2006;

Luật An toàn thông tin mạng năm 2015;

Luật An ninh mạng năm 2018;

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 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 về ban hành quy định về hệ thống phương án ứng phó khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Thông tư số 03/2017/TT-BTTTT ngày 24/04/2017 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;

Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông quy định về điều phối, ứng phó sự cố an toàn thông tin mạng trên toàn quốc;

Quyết định số 468/QĐ-UBND ngày 06/6/2017 của UBND tỉnh Gia Lai về việc ban hành Quy định về ứng phó sự cố an toàn thông tin mạng trên địa bàn tỉnh Gia Lai.

Nhằm tăng cường công tác bảo đảm an toàn thông tin mạng trên địa bàn tỉnh, UBND tỉnh Gia Lai xây dựng Kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Gia Lai với những nội dung cụ thể như sau:

II. MỤC ĐÍCH, YÊU CẦU:

1. Mục đích:

- Bảo đảm an toàn thông tin mạng trên địa bàn 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 mạng. Đề ra các giải pháp ứng phó khi gặp sự cố mất an toàn thông tin mạng.

- Tạo chuyển biến mạnh mẽ trong nhận thức về an toàn thông tin đối với lực

lượng cán bộ, công chức, viên chức.

- Bảo đảm 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:

- 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 phó sự cố tương ứng, kịp thời, phù hợp.

- Phương án đối phó, ứng phó 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.

III. NỘI DUNG KẾ HOẠCH:

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.

1.1. Nội dung: Tổ chức tuyên truyền, phổ biến trên các phương tiện thông tin đại chúng, Cổng thông tin điện tử của tỉnh, các Trang thông tin điện tử thành viên, lồng ghép vào các hội nghị của tỉnh về công nghệ thông tin (CNTT) về Luật An ninh mạng; 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 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 phó 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 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 phó sự cố an toàn thông tin mạng trên toàn quốc; Quyết định số 468/QĐ-UBND ngày 06/6/2017 của UBND tỉnh Gia Lai về việc ban hành Quy định về ứng phó sự cố an toàn thông tin mạng trên địa bàn tỉnh Gia Lai.

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

1.3. Đơn vị phối hợp: Các sở, ban, ngành; UBND các huyện, thị xã, thành phố; các đơn vị có liên quan của tỉnh; các cơ quan thông tấn, báo chí.

1.4. Thời gian thực hiện: Trong năm 2018 và các năm tiếp theo.

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

2.1. Nội dung: Tổ chức đánh giá hiện trạng và khả năng bảo đảm an toàn thông tin mạng của các hệ thống thông tin dùng chung của tỉnh và của các đơn vị, địa phương trong tỉnh; đánh giá, dự báo các nguy cơ, sự cố, tấn công mạng và đề ra các giải pháp bảo đảm an toàn thông tin cho các hệ thống thông tin.

2.2 Đơn vị chủ trì: Sở Thông tin và Truyền thông; các sở, ban ngành; UBND các huyện, thị xã, thành phố.

2.3. 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; Nhà cung cấp dịch vụ thông tin mạng; các đơn vị liên quan khác.

2.4. Thời gian thực hiện: Thường xuyên hàng năm.

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

3.1. Nội dung: 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 cần đảm bảo các nội dung sau:

- 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, cơ sở dữ liệu, 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...

- 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, cơ sở dữ liệu, 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...

- 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.

- 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.

3.2. Trách nhiệm xây dựng phương án:

- Ủy quyền cho Sở Thông tin và Truyền thông xây dựng và ban hành Phương án đối phó, ứng cứu sự cố an toàn thông tin mạng của tỉnh. Đối với các hệ thống thông tin dùng chung của tỉnh, Sở Thông tin và Truyền thông chủ trì, phối hợp với các đơn vị liên quan 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 đánh giá, 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.

- Các cơ quan, đơn vị, địa phương xây dựng phương án đối phó, ứng cứu sự cố các hệ thống thông tin ở cơ quan, đơn vị, địa phương mình.

- Các đơn vị cung cấp dịch vụ thông tin có trách nhiệm phối hợp trong việc xây dựng các phương án nêu trên.

3.3. Thời gian thực hiện: Từ năm 2018 và bổ sung hàng năm.

4. Triển khai 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.

4.1. Triển khai các chương trình huấn luyện, diễn tập:

- Nội dung: Thực hiện 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.

- Đơn vị phối hợp: Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh; Đơn vị vận hành hệ thống thông tin *(các sở, ban ngành; UBND các huyện, thị xã, thành phố)*, Cơ quan điều phối an ninh mạng quốc gia *(Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam - VNCERT)*; các đơn vị chức năng liên quan; các nhà cung cấp dịch vụ thông tin.

- **Thời gian thực hiện**: Hàng năm.

4.2. Phòng ngừa sự cố và phát hiện sớm sự cố:

- **Nội dung:** Trang bị, nâng cấp thiết bị, công cụ, phương tiện, gia hạn bản quyền phần mềm phục vụ ứng cứu, khắc phục sự cố; chuẩn bị các điều kiện bảo đảm, sẵn sàng đối phó, ứng cứu, khắc phục khi sự cố xảy ra; tổ chức, duy trì hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh; thuê dịch vụ kỹ thuật và tổ chức tham gia các hoạt động của mạng lưới ứng cứu 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 hệ thống thông tin *(các sở, ban ngành; UBND các huyện, thị xã, thành phố)*, Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh.

- **Đơn vị phối hợp**: Cơ quan điều phối an ninh mạng 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 hàng năm.

5. 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 về 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)*.

5.1. 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 hệ thống thông tin *(các sở, ban, ngành; UBND các huyện, thị xã, thành phố)* báo cáo Chủ quản hệ thống thông tin, Sở Thông tin và Truyền thông, đồng gửi 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 Chủ quản hệ thống thông tin, Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam – VNCERT, Ban Chỉ đạo ứng dụng CNTT tỉnh (*hoặc* Ban Chỉ đạo xây dựng chính quyền điện tử / Ban Chỉ đạo ứng cứu sự cố của tỉnh) và các cơ quan có liên quan;

+ Ban Chỉ đạo ứng dụng CNTT tỉnh (*hoặc* Ban Chỉ đạo xây dựng chính quyền điện tử / Ban Chỉ đạo ứng cứu sự cố của tỉnh) báo cáo Cơ quan thường trực và Ban Chỉ đạo quốc gia về ứng cứu sự cố.

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

5.2. 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 hệ thống thông tin (*các sở, ban, ngành; UBND các huyện, thị xã, thành phố)*; Đội ứng cứu sự cố bảo đảm an toàn thông tin mạng của tỉnh.

- **Đơn vị phối hợp:** Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam - VNCERT; tổ chức, cá nhân gửi thông báo, báo cáo sự cố; đơn vị cung cấp dịch vụ thông tin mạng; 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.

5.3. 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:

- **Nội dung:** Các cơ quan, đơn vị, địa phương bố trí 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.

- **Đơn vị thực hiện:** Sở Thông tin và Truyền thông; Đơn vị vận hành hệ thống thông tin *(các sở, ban ngành; UBND các huyện, thị xã, thành phố)*, Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh.

- **Đơn vị phối hợp:** Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam - VNCERT; tổ chức, cá nhân gửi thông báo, báo cáo sự cố; đơn vị cung cấp dịch vụ thông tin mạng; các đơn vị chức năng liên quan.

- **Thời gian thực hiện:** Trong quá trình ứng phó sự cố về an toàn thông tin mạng.

6. Đào tạo, bồi dưỡng kiến thức chuyên sâu về bảo đảm an toàn thông tin mạng:

- **Nội dung:** Xây dựng kế hoạch bồi dưỡng, đào tạo chuyên sâu về bảo đảm an toàn thông tin mạng, phòng chống tấn công mạng, phòng ngừa mã độc,... cho đội ngũ cán bộ vận hành, quản trị hệ thống mạng và cơ sở dữ liệu của các đơn vị gồm: Trung tâm Công nghệ thông tin và Truyền thông, Phòng Công nghệ thông tin thuộc Sở Thông tin và Truyền thông; Phòng Cơ yếu thuộc Văn phòng Tỉnh ủy; Trung tâm Tin học thuộc Văn phòng UBND tỉnh.

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

- **Đơn vị phối hợp:** Văn phòng Tỉnh ủy; Văn phòng UBND tỉnh; Sở Nội vụ; Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam - VNCERT; Cục An toàn thông tin - Bộ TT&TT, các đơn vị có liên quan khác.

- **Thời gian thực hiện:** Thường xuyên hàng năm.

VI. KINH PHÍ THỰC HIỆN:

Kinh phí thực hiện kế hoạch được sử dụng từ nguồn ngân sách tỉnh và các nguồn kinh phí hợp pháp khác.

V. TỔ CHỨC THỰC HIỆN:

1. Các sở, ban, ngành, UBND các huyện, thị xã, thành phố và các đơn vị liên quan:

- 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, địa phương mình để triển khai 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. Cử lãnh đạo phụ trách hoặc cán bộ phụ trách CNTT tham gia diễn tập ứng phó sự cố của tỉnh.

- Thực hiện xác định cấp độ, lập hồ sơ đề xuất cấp độ an toàn hệ thống thông tin theo quy định tại 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 24/04/2017 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 thực hiện các nhiệm vụ được giao trong Kế hoạch này và các nhiệm vụ phát sinh khi có sự cố an toàn thông tin mạng.

- Định kỳ hàng năm hoặc đột xuất báo cáo kết quả ứng phó sự cố bảo đảm an toàn thông tin mạng trên địa bàn tỉnh về Sở Thông tin và Truyền thông *(theo đề cương hướng dẫn của Sở Thông tin và Truyền thông)* để tổng hợp báo cáo các cơ quan cấp trên.

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; 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, tổ chức triển khai, đôn đốc, kiểm tra, đánh giá, giám sát công tác bảo đảm an toàn thông tin định kỳ hằng 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 24/04/2017 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 xây dựng kế hoạch, phương án và thực hiện ứng cứu sự cố bảo đảm an toàn thông tin mạng ở các sở, ban, ngành, UBND các huyện, thị xã, thành phố. Chỉ đạo các doanh nghiệp cung cấp dịch vụ thông tin trên mạng ở địa bàn tỉnh phối hợp với các đơn vị, địa phương trong việc đảm bảo an toàn thông tin mạng.

- 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 bảo đảm cho hoạt động của Ban Ban chỉ đạo Ứng dụng Công nghệ thông tin của tỉnh *(đảm nhiệm chức năng ứng cứu khẩn cấp sự cố an toàn thông tin mạng của tỉnh)*, 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.

- Định kỳ hàng năm hoặc đột xuất lập báo cáo kết quả thực hiện ứng phó sự cố bảo đảm an toàn thông tin mạng trên địa bàn tỉnh gửi UBND tỉnh và Bộ Thông tin và Truyền thông theo quy định.

3. Sở Kế hoạch và Đầu tư; Sở Tài chính:

Căn cứ các nội dung, nhiệm vụ trong Kế hoạch này để thẩm định, tham mưu UBND tỉnh xem xét bố trí ngân sách nhà nước hằng năm cho các cơ quan, đơn vị đảm bảo triển khai thực hiện có hiệu quả Kế hoạch đề ra.

4. Công an tỉnh; Bộ Chỉ huy Quân sự tỉnh:

- Tổ chức, chỉ đạo, triển khai công tác phòng, chống, điều tra tội phạm lợi dụng hệ thống mạng để xâm phạm an ninh quốc gia, gây mất an toàn thông tin mạng, mất trật tự an toàn xã hội.

- Phối hợp với Sở Thông tin và Truyền thông kiểm tra, xử lý các vi phạm về an toàn thông tin mạng theo quy định.

Trên đây là Kế hoạch Ứng phó sự cố bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Gia Lai, yêu cầu Thủ trưởng các sở, ban, ngành; Chủ tịch UBND các huyện, thị xã, thành phố và các đơn vị liên quan nghiêm túc triển khai thực hiện. Trong quá trình thực hiện nếu có vướng mắc, khó khăn, các đơn vị, địa phương phản ánh kịp thời về Sở Thông tin và Truyền thông để tổng hợp báo cáo UBND tỉnh chỉ đạo, giải quyết./.

Nơi nhận:
- Bộ Thông tin và Truyền thông (b/c);
- TTr. Tỉnh ủy;
- TTr. HĐND tỉnh;
- Chủ tịch, các Phó Chủ tịch UBND tỉnh;
- Ban Chỉ đạo ứng dụng CNTT của tỉnh;
- Các sở, ban, ngành thuộc tỉnh (để thực hiện);
- UBND các huyện, thị xã, thành phố (để thực hiện);
- Các dn Viễn thông trên địa bàn tỉnh (để thực hiện);
- Cổng thông tin điện tử tỉnh;
- CVP, các PCVP UBND tỉnh;
- Lưu: VT, NC, KTTH, KGVX.

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

Huỳnh Nữ Thu Hà