

**KẾ HOẠCH**  
**Ứng phó sự cố, đảm bảo an toàn thông tin mạng**  
**trên địa bàn huyện Khánh Sơn năm 2018**

Căn cứ Kế hoạch số 439/KH-UBND ngày 11/01/2018 của UBND tỉnh Khánh Hòa về ứng phó sự cố, đảm bảo an toàn thông tin mạng trên địa bàn huyện Khánh Sơn năm 2018. UBND huyện Khánh Sơn xây dựng Kế hoạch ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn huyện Khánh Sơn năm 2018 gồm những nội dung cụ thể như sau:

**I. MỤC ĐÍCH, YÊU CẦU**

**1. Mục đích**

Đảm bảo an toàn thông tin cho các hệ thống thông tin quan trọng trên địa bàn huyện; chủ động đề ra các giải pháp ứng phó với sự cố mất an toàn thông tin mạng, huy động mọi nguồn lực xã hội vào công tác phòng, chống tấn công mạng và khắc phục nhanh chóng các sự cố mất an toàn thông tin mạng.

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

**2. Yêu cầu**

Có 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.

Quá trình triển khai thực hiện các cơ quan chức năng phải đảm bảo đúng pháp luật, đúng quy trình chuyên môn, khả thi, hiệu quả.

**II. NHIỆM VỤ TRIỂN KHAI**

**1. Triển khai các nhiệm vụ khi chưa có sự cố xảy ra**

Tổ chức Hội nghị tuyên truyền, phổ biến Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 và các văn bản quy phạm pháp luật về an toàn thông tin mạng trong tháng 4/2018.

Tổ chức tuyên truyền phổ biến Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 và các văn bản quy phạm pháp luật về an toàn thông tin mạng trên các phương tiện thông tin đại chúng, tài liệu tuyên truyền, Cổng thông tin điện tử huyện thường xuyên trong năm.

**1.2. Tham gia các chương trình huấn luyện, diễn tập**

Tham gia các chương trình huấn luyện, diễn tập các phương án đối phó, ứng cứu sự cố tương ứng với các kịch bản, tình huống cụ thể; tham gia các chương trình 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 an toàn thông tin mạng do Sở Thông tin và Truyền thông tổ chức trong quý II năm 2018.

### **1.3. Triển khai phòng ngừa sự cố, giám sát phát hiện sớm sự cố**

Văn phòng HĐND&UBND huyện phối hợp với các cơ quan liên quan thực hiện giám sát, phát hiện sớm các nguy cơ, sự cố mất an toàn thông tin đề nghị Đội Ứng cứu sự cố mạng máy tính tỉnh Khánh Hòa phối hợp xử lý; tuyên truyền nâng cao nhận thức về nguy cơ, sự cố, tấn công mạng định kỳ hàng quý.

### **1.4 Đánh giá các nguy cơ, sự cố an toàn thông tin mạng**

Văn phòng HĐND&UBND huyện phối hợp với các cơ quan liên quan tổ chức đánh giá hiện trạng và khả năng bảo đảm an toàn thông tin mạng của các hệ thống thông tin; 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 định kỳ hàng quý.

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

Văn phòng HĐND&UBND huyện phối hợp với các cơ quan 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 thường xuyên trong năm đảm bảo các nội dung:

a) Phương pháp, cách thức để xác định nhanh chóng, kịp thời về 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...

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 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 người quản trị, vận hành hệ thống:
  - + 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 dùng 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.

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.

## **2. Triển khai các nhiệm vụ khi có sự cố xảy ra**

### **2.1. Tiếp nhận, phân tích, ứng cứu ban đầu và thông báo sự cố**

a) Văn phòng HĐND&UBND huyện phối hợp với các cơ quan liên quan tiếp nhận, xác minh sự cố: Theo dõi, tiếp nhận, phân tích các cảnh báo dấu hiệu sự cố có thể từ các nguồn bên trong và bên ngoài; tổ chức ghi nhận, thu thập chứng cứ, xác định nguồn gốc sự cố.

b) Văn phòng HĐND&UBND huyện phối hợp với các cơ quan liên quan triển khai các bước ưu tiên ứng cứu ban đầu: tổ chức triển khai các bước ưu tiên ban đầu để xử lý sự cố theo kế hoạch.

c) Văn phòng HĐND&UBND huyện phối hợp với các cơ quan liên quan triển khai lựa chọn phương án ứng cứu: căn cứ kế hoạch để lựa chọn phương án ngăn chặn và xử lý sự cố; báo cáo đề xuất cơ quan cấp trên xin ý kiến chỉ đạo nếu cần.

d) Văn phòng HĐND&UBND huyện phối hợp với các cơ quan liên quan chỉ đạo sự cố nêu trên: căn cứ theo báo cáo, đề xuất phối hợp với chủ quản hệ thống thông tin, tham khảo ý kiến và phối hợp với cơ quan cấp triển khai công tác ứng cứu, xử lý sự cố.

đ) Văn phòng HĐND&UBND huyện phối hợp với các cơ quan liên quan báo cáo sự cố: báo cáo sự cố đến các tổ chức, cá nhân liên quan bên trong và bên ngoài cơ quan, tổ chức theo quy định.

## **2.2 Triển khai ứng cứu, ngăn chặn và xử lý sự cố**

Văn phòng HĐND&UBND huyện phối hợp với các cơ quan liên quan triển khai thu thập chứng cứ, phân tích, xác định phạm vi, đối tượng bị ảnh hưởng; phân tích, xác định nguồn gốc tấn công, tổ chức ứng cứu và ngăn chặn, giảm thiểu tác động, thiệt hại đến hệ thống thông tin.

## **2.3. Xử lý sự cố, gỡ bỏ và khôi phục**

a) Xử lý sự cố: sau khi đã triển khai ngăn chặn sự cố, Văn phòng HĐND&UBND huyện phối hợp với các cơ quan liên quan triển khai tiêu diệt, gỡ bỏ các mã độc, phần mềm độc hại, khắc phục các điểm yếu an toàn thông tin của hệ thống thông tin.

b) Khôi phục: Văn phòng HĐND&UBND huyện phối hợp với các cơ quan liên quan triển khai các hoạt động khôi phục hệ thống thông tin, dữ liệu và kết nối, cấu hình hệ thống an toàn; bổ sung các thiết bị, phần mềm bảo đảm an toàn thông tin cho hệ thống thông tin.

c) Kiểm tra, đánh giá hệ thống thông tin: Văn phòng HĐND&UBND huyện phối hợp với các cơ quan liên quan triển khai kiểm tra, đánh giá hoạt động của toàn bộ hệ thống thông tin sau khi khắc phục sự cố. Trường hợp hệ thống chưa hoạt động ổn định, cần tiếp tục tổ chức thu thập, xác minh lại nguyên nhân và tổ chức các bước tương ứng tại Khoản 2.2 và Khoản 2.3 của Kế hoạch này để dứt điểm, khôi phục hoạt động bình thường của hệ thống thông tin.

## **2.4. Tổng kết, đánh giá**

Văn phòng HĐND&UBND huyện phối hợp với các cơ quan liên quan triển khai tổng hợp lại toàn bộ các thông tin, báo cáo, phân tích có liên quan đến sự cố, công tác triển khai phương án ứng cứu sự cố, báo cáo cơ quan cấp trên; tổ chức 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.

## **III. KINH PHÍ THỰC HIỆN**

Các cơ quan được giao thực hiện các nhiệm vụ tại Mục II của Kế hoạch này chủ động xây dựng dự toán kinh phí chi tiết gửi UBND huyện (qua Phòng VH TT) đề tổng hợp gửi cơ quan có thẩm quyền phê duyệt, cấp kinh phí.

## **IV. TỔ CHỨC THỰC HIỆN**

### **1. Các cơ quan, đơn vị, UBND các xã, thị trấn; Công an huyện**

Thủ trưởng các cơ quan, đơn vị, địa phương và Trưởng Công an huyện căn cứ vào tình hình thực tế tại cơ quan, đơn vị, địa phương mình triển khai thực hiện có hiệu quả nội dung Kế hoạch này.

Thực hiện bố trí cán bộ, công chức công tác đảm bảo an toàn thông tin tại cơ quan, địa phương mình; kịp thời thông báo về Phòng Văn hóa và Thông tin huyện khi có sự thay đổi cán bộ công chức tham mưu công tác đảm bảo an toàn thông tin mạng của cơ quan, đơn vị.

Tích cực phối hợp với các cơ quan, đơn vị chủ trì thực hiện các nhiệm vụ được giao theo Kế hoạch này

### **2. Phòng Văn hóa và Thông tin huyện**

Tham mưu UBND huyện xây dựng và triển khai Kế hoạch Ứng phó sự cố, đảm bảo an toàn thông tin mạng trên địa bàn huyện hàng năm.

Theo dõi, đôn đốc, phối hợp với các cơ quan, đơn vị, UBND các xã, thị trấn; Công an huyện trong việc triển khai thực hiện Kế hoạch này; định kỳ hàng năm báo cáo kết quả thực hiện cho UBND huyện để theo dõi, xem xét và chỉ đạo.

### **3. Phòng Tài chính – Kế hoạch huyện**

Thực hiện bố trí kinh phí cho các cơ quan, đơn vị để thực hiện các nội dung tại Điểm 1 Mục 2 theo Kế hoạch này.

### **4. Văn phòng HĐND&UBND huyện**

Căn cứ nhiệm vụ được giao tại Mục II Kế hoạch này, phối hợp với các cơ quan liên quan tham mưu UBND huyện xây dựng dự toán kinh phí chi tiết gửi Sở Thông tin và Truyền thông trình cơ quan có thẩm quyền phê duyệt.

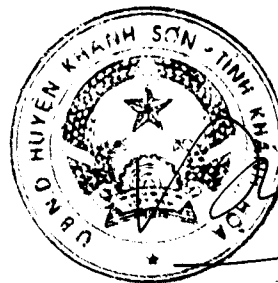
Trên đây là Kế hoạch ứng phó sự cố, đảm bảo an toàn thông tin mạng trên địa bàn huyện Khánh Sơn năm 2018./.

#### **Nơi nhận:**

- Sở Thông tin và Truyền thông tỉnh;
- TT Huyện ủy;
- Các cơ quan, đơn vị huyện ;
- UBND các xã, thị trấn;
- Lưu: VT, PVHTT.

*nu*

**TM. ỦY BAN NHÂN DÂN**



**CHỦ TỊCH**

*Đinh Ngọc Bình*  
**Đinh Ngọc Bình**