UBND TỈNH KHÁNH HÒA **THANH TRA TỈNH**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số:29 /KH-TTT	*Khánh Hòa, ngày 09 tháng 6 năm 2025*

KẾ HOẠCH
Ứng phó sự cố đảm bảo an toàn thông tin mạng của Thanh tra tỉnh

Thực hiện Kế hoạch số 5479/KH-UBND ngày 08/5/2025 của UBND tỉnh về Ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Khánh Hòa năm 2025; Thanh tra tỉnh xây dựng Kế hoạch ứng phó sự cố đảm bảo an toàn thông tin mạng của Thanh tra tỉnh như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích:

- Đảm bảo an toàn thông tin mạng của Thanh tra tỉnh, trong đó tập trung đảm bảo an toàn thông tin cho các hệ thống thông tin quan trọng của cơ quan, 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.

- Tạo chuyển biến mạnh mẽ trong nhận thức về an toàn thông tin đối với công chức, người lao động thuộc Thanh tra tỉnh.

- Đảm bảo 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:

- 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.

- 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:

1.1. Nội dung:

- Tuyên truyền, phổ biến trên Trang thông tin điện tử của Thanh tra tỉnh, lồng ghép vào Ngày pháp luật định kỳ của cơ quan về Luật an ninh mạng và các quy định về công tác ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng.

1.2. Đơn vị chủ trì: Văn phòng.

1.3. Đơn vị phối hợp: Các phòng thuộc Thanh tra tỉnh;

1.4. Thời gian thực hiện: Trong năm 2025 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 hệ thống thông tin trong cơ quan *(hệ thống thư điện tử, hệ thống trang thông tin điện tử, hệ thống dịch vụ công trực tuyến, hệ thống phần mềm một cửa điện tử, hệ thống quản lý văn bản điều hành)*; đánh giá, dự báo các nguy cơ, sự cố, tấn công mạng và đề ra các giải pháp đảm bảo an toàn thông tin cho các hệ thống thông tin mạng máy tính nội bộ (LAN) của Thanh tra tỉnh.

2.2. Đơn vị chủ trì: Văn phòng.

2.3. Đơn vị phối hợp: Các phòng thuộc Thanh tra tỉnh.

2.4. Thời gian thực hiện: Thực hiện 01 cuộc đánh giá/năm

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

3.1. Nội dung:

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...;

- 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:

Tình huống sự cố do bị tấn công mạng; tình huống sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật; tình huống sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn v.v...

3.2. Đơn vị chủ trì: Văn phòng.

3.3. Đơn vị phối hợp: Các phòng thuộc Thanh tra tỉnh; Công an tỉnh.

3.4. Thời gian thực hiện: Hàng năm.

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

- Đầu tư, quản lý, khai thác các trang thiết bị thiết yếu bảo đảm an toàn thông tin cho cơ quan, đơn vị gồm: Thiết bị tường lửa mạng (Network fire wall), thiết bị phục vụ quản trị, giám sát an ninh mạng…

- Sử dụng phần mềm virus có bản quyền quản lý tập trung (Endpoint security) đáp ứng yêu cầu bảo vệ máy tính và giám sát an ninh cho 100% máy tính trong mạng của cơ quan, đơn vị theo hướng ưu tiên sử dụng các giải pháp phần mềm virus có bản quyền quản lý tập trung trong nước như: BKAV EndPoint Securit.

- Đầu tư trang thiết bị, phần mềm bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố; 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; thuê dịch vụ kỹ thuật và tổ chức tham gia các hoạt động của mạng lưới ứng cứu sự cố.

- *Đơn vị chủ trì*: Văn phòng.

- *Đơn vị phối hợp*: Các phòng thuộc Thanh tra tỉnh.

- *Thời gian thực hiện*: Hàng năm.

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

5. 1. Tiếp nhận, xác định sự cố:

Thành viên đội ứng cứu sự cố an toàn thông tin mạng của tỉnh tại Thanh tra tỉnh tiếp nhận, phân tích các cảnh báo, dấu hiệu sự cố từ các nguồn bên trong và bên ngoài (cảnh báo sự cố: Văn bản, email, điện thoại, website, facebook, mạng xã hội...; phát hiện sự cố thông qua kiểm tra, rà soát, đánh giá). Khi xác định được sự cố đã xảy ra, cần tổ chức ghi nhận, thu thập chứng cứ, xác định 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;

- 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,...

5.2. Triển khai các bước ưu tiên ứng cứu ban đầu

- Xác định sự cố xảy ra, thành viên đội ứng phó sự cố an toàn thông tin của Thanh tra tỉnh triển khai các bước ưu tiên ban đầu để xử lý sự cố theo phương án, kế hoạch ứng phó sự cố đã được cấp thẩm quyền phê duyệt/xác nhận hoặc theo tư vấn, hướng dẫn của Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh và Công an tỉnh.

- Đội ứng cứu sự cố phải kịp thời phân tích và xác định tình hình sự cố để xác định phạm vi ảnh hưởng. Những phân tích ban đầu sẽ cung cấp thông tin cho các hoạt động tiếp theo.

5.3 Ngăn chặn, xử lý sự cố

- Đơn vị vận hành hệ thống phối hợp với thành viên Đội ứng cứu sự cố và các đơn vị liên quan báo cáo, đề xuất cơ quan chủ quản hệ thống thông tin, Đội ứng cứu sự cố phê duyệt phương án, chiến lược ngăn chặn và xử lý sự cố và đề nghị hỗ trợ từ Cơ quan điều phối quốc gia nếu cần thiết.

5.4. Xác định nguồn gốc tấn công

-Thành viên Đội ứng cứu sự cố triển khai phân tích, xác định nguồn gốc tấn công để ngăn chặn, giảm thiểu tác động, thiệt hại đến hệ thống thông tin.

5.5. Khắc phục, gỡ bỏ sự cố

- Sau khi đã triển khai ngăn chặn sự cố, phải tiến hành tiêu diệt các mã độc, phần mềm độc hại, khắc phục các điểm yếu ATTT của hệ thống (xây dựng lại hệ thống, thay thế các tệp tin bị lỗi, cài đặt các bản vá lỗi, thay đổi mật khẩu và rà soát các chính sách ATTT).

5.6 . Khôi phục

Triển khai các hoạt động khôi phục hệ thống, dữ liệu và kết nối (phải khôi phục từ các bản sao lưu hệ thống "sạch"); cấu hình hệ thống an toàn; bổ sung các thiết bị, phần cứng, phần mềm bảo đảm ATTT cho hệ thống thông tin và kiểm tra thử toàn bộ hệ thống sau khi khắc phục sự cố.

III. KINH PHÍ THỰC HIỆN

Kinh phí thực hiện được sử dụng từ nguồn ngân sách.

IV. TỔ CHỨC THỰC HIỆN

1. Văn phòng:

- Xây dựng nội dung, lập dự toán kinh phí lồng ghép trong Kế hoạch ứng dụng CNTT hàng năm của cơ quan 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.

- Thực hiện theo công văn số: 845/STTTT-CNTT ngày 20/4/2021 về kết quả đề xuất cấp độ an toàn hệ thống thông tin (cấp độ 1).

- Thực hiện theo Quyết định số 07/QĐ-TTT ngày 01/4/ 2022 của Thanh tra tỉnh.

2. Các phòng thuộc Thanh tra tỉnh:

- Phối hợp với Văn phòng kiểm tra, xử lý các vấn đề về an toàn thông tin mạng khi có yêu cầu.

- Hỗ trợ Văn phòng đánh giá nguy cơ mất an toàn thông tin mang khi có yêu cầu.

Trên đây là Kế hoạch ứng phó sự cố đảm bảo an toàn thông tin mạng của Thanh tra tỉnh năm 2025; yêu cầu Văn phòng, các phòng, công chức thuộc Thanh tra tỉnh nghiêm túc triển khai thực hiện./.

Nơi nhận: (VBĐT)
- Công an tỉnh;
- LĐ TTT;
- Trưởng các phòng;
- Trang TTĐT (đăng tin);
- Lưu: VT, KT.

KT. CHÁNH THANH TRA
PHÓ CHÁNH THANH TRA

Trương Thanh Phong