| | |
|---|---|
| UBND TỈNH BÌNH ĐỊNH<br>**THANH TRA TỈNH** | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**<br>**Độc lập – Tự do – Hạnh phúc** |
| Số: 645 /PA-TTT | *Bình Định, ngày 30 tháng 8 năm 2023* |

# PHƯƠNG ÁN
## Phối hợp ứng phó sự cố, đảm bảo an toàn thông tin mạng trong hoạt động của Thanh tra tỉnh

Để bảo đảm an toàn thông tin cho hệ thống thông tin của Thanh tra tỉnh theo cấp độ 2 (được phê duyệt theo Quyết định số 748/QĐ-TTT ngày 30/9/2021 của Chánh Thanh tra tỉnh); bảo đảm 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, bảo đảm nguồn lực và các điều kiện cần thiết để ứng phó sự cố an toàn thông tin mạng tại cơ quan, Thanh tra tỉnh ban hành Phương án phối hợp ứng phó sự cố, bảo đảm an toàn thông tin mạng trong hoạt động của cơ quan với những nội dung sau:

## Chương I
## CÁC QUY ĐỊNH CHUNG

**Điều 1.** Phạm vi điều chỉnh, đối tượng áp dụng

Phương án này áp dụng đối với các phòng và toàn thể công chức, người lao động thuộc Thanh tra tỉnh và các cá nhân khác liên quan trong việc phối hợp ứng phó sự cố, bảo đảm an toàn thông tin mạng (ATTT) trong hoạt động của Thanh tra tỉnh.

**Điều 2.** Điều kiện, nguyên tắc chung, nguyên tắc ưu tiên để duy trì hoạt động của hệ thống khi triển khai ứng cứu sự cố; phương châm ứng phó sự cố

- Tuân thủ các quy định pháp luật về điều phối, ứng cứu sự cố an toàn thông tin mạng.

- Chủ động, kịp thời, nhanh chóng, chính xác, đồng bộ và hiệu quả.

- Phối hợp chặt chẽ, chính xác, đồng bộ và hiệu quả giữa cơ quan với Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh, Sở Thông tin và Truyền thông.

**Điều 3.** Lực lượng tham gia ứng phó sự cố

- Cơ quan Thanh tra tỉnh là đơn vị vận hành hệ thống thông tin.

- Sở Thông tin và Truyền thông: là cơ quan thường trực của Đội ứng cứu sự cố ATTT mạng của tỉnh.

- Đội ứng cứu sự cố ATTT mạng của tỉnh.

- Đơn vị được thuê dịch vụ về CNTT (nếu cần thiết).

**Điều 4.** Chức năng, nhiệm vụ, trách nhiệm và cơ chế, quy trình phối hợp giữa Thanh tra tỉnh và các đơn vị phối hợp

- Thanh tra tỉnh có trách nhiệm theo dõi thường xuyên việc đảm bảo ATTT mạng và báo cáo lãnh đạo cơ quan chỉ đạo phối hợp các đơn vị ứng cứu khi có sự cố xảy ra.

- Sở Thông tin và Truyền thông thực hiện công tác điều phối, giám sát cơ chế phối hợp, chia sẻ thông tin theo phạm vi, chức năng, nhiệm vụ của mình để huy động nguồn lực ứng cứu sự cố.

- Đội ứng cứu sự cố ATTT mạng của tỉnh cử thành viên và tham gia hoạt động ứng cứu theo Quy chế hoạt động của Đội ứng cứu sự cố ATTT mạng của tỉnh.

- Đơn vị được thuê dịch vụ về CNTT: phối hợp, hỗ trợ khắc phục lỗi, sự cố nhỏ (nếu có) hoặc sự cố liên quan đến đường truyền, thiết bị.

## Chương II
## ĐÁNH GIÁ CÁC NGUY CƠ, SỰ CỐ AN TOÀN THÔNG TIN MẠNG

**Điều 5.** Đánh giá các nguy cơ, sự cố an toàn thông tin mạng

1. Đánh giá hiện trạng và khả năng đảm bảo ATTT mạng của hệ thống thông tin cần được bảo vệ.

2. Đánh giá, dự báo các nguy cơ, sự cố, tấn công mạng có thể xảy ra với đối với hệ thông thông tin và các đối tượng cần bảo vệ.

3. Đánh giá, dự báo các hậu quả, thiệt hại, tác động có thể có nếu xảy ra sự cố.

4. 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 cả những đơn vị được thuê cung cấp dịch vụ về bảo mật, CNTT nếu có).

## Chương III
## PHƯƠNG ÁN PHỐI HỢP ỨNG PHÓ SỰ CỐ ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

**Điều 6.** Xây dựng phương án phối hợp ứng phó sự cố ATTT mạng

Phương án phối hợp ứng phó sự cố ATTT mạng phải nhanh chóng xác định được tính chất, mức độ nghiêm trọng của sự cố khi có sự cố xảy ra. Việc xây dựng phương án đối phó, ứng cứu sự cố cần đảm bảo các nội dung sau:

1. Phát hiện, tiếp nhận, xác định nguyên nhân, nguồn gốc của sự cố

Văn phòng là đầu mối vận hành hệ thống thông tin của Thanh tra tỉnh phát hiện sự cố thông qua kiểm tra, rà soát, đánh giá hoặc tiếp nhận sự cố từ Văn bản, email, điện thoại, website, mạng xã hội... 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.

Các loại sự cố chính, bao gồm:

- Sự cố do bị 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....

2. 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

Sau khi đã xác định sự cố xảy ra, căn cứ vào tính chất của sự cố, bộ phận vận hành hệ thống thông tin cơ quan triển khai các bước ưu tiên ban đầu để xử lý sự cố tại chỗ (nếu có thể) hoặc theo sự hỗ trợ, hướng dẫn của Đội ứng cứu sự cố của tỉnh, tư vấn của đơn vị được thuê dịch vụ về CNTT.

3. Xử lý sự cố và khôi phục

Sau khi đã triển khai ngăn chặn sự cố, bộ phận vận hành hệ thống thông tin phối hợp với cơ quan thường trực về ứng cứu sự cố của tỉnh và các đơn vị 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.

Văn phòng Thanh tra tỉnh chủ trì phối hợp với các đơn vị 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 cứng phần mềm bảo đảm an toàn thông tin cho hệ thống thông tin.

4. Kiểm tra, đánh giá hệ thống thông tin

Thanh tra tỉnh và các đơn vị 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 để xử lý dứt điểm, khôi phục hoạt động bình thường của hệ thống thông tin.

Thanh tra tỉnh phối hợp với Đơn vị thường trực về ứng cứu sự cố của tỉnh triển khai tổng hợp và xây dựng báo cáo kết thúc ứng phó sự cố, trong đó trình bày chi tiết quá trình xử lý sự cố, tóm tắt tổng quát về tình hình sự cố và đề xuất cách thức triển khai điều phối, ứng cứu sự cố nhằm xử lý nhanh, giảm nhẹ rủi ro và thiệt hại đối với sự cố tương tự.

5. Báo cáo đánh giá kết thúc ứng phó sự cố

Sau khi kết thúc ứng cứu sự cố, Văn phòng xây dựng báo cáo báo cáo kết thúc ứng phó sự cố, gửi về Cơ quan chuyên trách về an toàn thông tin của tỉnh.

## Chương IV
## TRIỂN KHAI CÁC BIỆN PHÁP PHÒNG NGỪA SỰ CỐ BẢO ĐẢM CÁC ĐIỀU KIỆN SẴN SÀNG ĐỐI PHÓ, ỨNG CỨU, KHẮC PHỤC SỰ CỐ

**Điều 7.** Thực hiện xây dựng các nội dung, nhiệm vụ cụ thể cần triển khai nhằm phòng ngừa sự cố bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố.

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

- Thực hiện nghiêm công tác phát hiện sớm nguy cơ về lỗ hổng bảo mật, các lỗi phần mềm do cơ quan chuyên môn cảnh báo và giám sát qua thiết bị hỗ trợ khác.

- 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.

- Tuyên truyền, nâng cao nhận thức về nguy cơ, sự cố, tấn công mạng.

- Cử công chức tham gia các chương trình đào tạo, bồi dưỡng kỹ năng đánh giả, ứng phó sự cố.

2. 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 phần mềm phục vụ ứng cứu, khắc phục sự cố; thuê dịch vụ bảo đảm an toàn thông tin.

- Chuẩn bị các nguồn lực để sẵn sàng đối phó, ứng cứu, khắc phục khi sự cố xảy ra.

## Chương V
## TỔ CHỨC THỰC HIỆN

**Điều 8.** Trách nhiệm của Văn phòng Thanh tra tỉnh.

- Là bộ phận chủ trì, phối hợp với các phòng thuộc Thanh tra tỉnh triển khai thực hiện các nội dung tại Điều 5, 6, 7 của Phương án này.

- Làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về ATTT mạng trong hoạt động của cơ quan.

3. Chủ trì, phối hợp với các phòng thuộc cơ quan tiến hành kiểm tra các công tác bảo đảm ATTT mạng định kỳ hoặc theo hướng dẫn của cơ quan chuyên môn.

4. Tham mưu đưa nội dung dự phòng kinh phí, nhân lực, vật lực 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 vào các kế hoạch về bảo đảm ATTT mạng, ứng dụng CNTT.

**Điều 9.** Trách nhiệm của các phòng thuộc cơ quan.

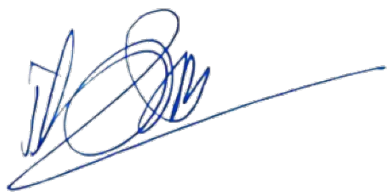
- Quan tâm, chú trọng đến công tác bảo đảm ATTT mạng trong quá trình sử dụng, khai thác thông tin trên mạng internet.

- Phối hợp phòng Văn phòng và các đơn vị liên quan khi cần thiết nhằm thực hiện công tác ứng phó khi có sự cố ATTT mạng trong hệ thống thông tin cơ quan.

Trong quá trình thực hiện Phương án này nếu có vấn đề vướng mắc, phát sinh, các phòng thuộc Thanh tra tỉnh phản ánh kịp thời về phòng Văn phòng để tổng hợp báo cáo Lãnh đạo chỉ đạo thực hiện./.

***Nơi nhận:***
- CTT, các PCTT;
- Các phòng thuộc cơ quan;
- Lưu: VT, VP.

**CHÁNH THANH TRA**



**Nguyễn Văn Thơm**