ỦY BAN NHÂN DÂN TỈNH HÀ TĨNH	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 1859 /QĐ-UBND	*Hà Tĩnh, ngày 07 tháng 8 năm 2023*

QUYẾT ĐỊNH
Về việc công bố thủ tục hành chính nội bộ giữa các cơ quan hành chính nhà nước thuộc phạm vi quản lý của Sở Thông tin và Truyền thông tỉnh Hà Tĩnh

CHỦ TỊCH ỦY BAN NHÂN DÂN TỈNH

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19/6/2015; Luật sửa đổi, bổ sung một số điều của Luật Tổ chức chính phủ và Luật Tổ chức chính quyền địa phương ngày 22/11/2019;

Căn cứ Quyết định số 1085/QĐ-TTg ngày 15/9/2022 của Thủ tướng Chính phủ về việc ban hành Kế hoạch rà soát, đơn giản hóa TTHC nội bộ trong hệ thống hành chính nhà nước giai đoạn 2022-2025;

Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Văn bản số 1200/STTTT-VP ngày 27/7/2023.

QUYẾT ĐỊNH:

Điều 1. Công bố kèm theo Quyết định này 01 (một) thủ tục hành chính nội bộ giữa các cơ quan hành chính nhà nước thuộc thẩm quyền giải quyết của Sở Thông tin và Truyền thông tỉnh Hà Tĩnh.

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

Điều 3. Chánh Văn phòng UBND tỉnh, Giám đốc các Sở, Thủ trưởng các ban, ngành cấp tỉnh; Chủ tịch UBND các huyện, thành phố, thị xã và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Văn phòng Chính phủ;
- Chủ tịch, các PCT UBND tỉnh;
- Chánh VP, các PCVP UBND tỉnh;
- Trung tâm CB-TH;
- Lưu: VT, NC_1.

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

ỦY BAN NHÂN DÂN TỈNH HÀ TĨNH

Lê Ngọc Châu

ỦY BAN NHÂN DÂN
TỈNH HÀ TĨNH

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

DANH MỤC VÀ NỘI DUNG QUY TRÌNH THỦ TỤC HÀNH CHÍNH NỘI BỘ GIỮA CÁC CƠ QUAN HÀNH CHÍNH NHÀ NƯỚC THUỘC THẨM QUYỀN GIẢI QUYẾT CỦA SỞ THÔNG TIN VÀ TRUYỀN THÔNG TỈNH HÀ TĨNH

(Ban hành kèm theo Quyết định số……/QĐ-UBND ngày / /2023 của Chủ tịch UBND tỉnh Hà Tĩnh)

PHẦN I: DANH MỤC THỦ TỤC HÀNH CHÍNH

TT	Tên thủ tục hành chính	Lĩnh vực	Cơ quan thực hiện
1	Thủ tục ứng cứu sự cố an toàn thông tin của các hệ thống thông tin/cơ sở dữ liệu (HTTT/CSDL) do tỉnh quản lý	Thông tin và Truyền thông	UBND tỉnh, Sở Thông tin và Truyền thông, Trung tâm CNTT và Truyền thông, Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Hà Tĩnh

PHẦN II: NỘI DUNG THỦ TỤC HÀNH CHÍNH NỘI BỘ

1. Thủ tục ứng cứu sự cố an toàn thông tin của các hệ thống thông tin/cơ sở dữ liệu (HTTTT/CSDL) do tỉnh quản lý.

- Trình tự thực hiện:

1. Phân tích và thông báo sự cố

1.1. Tiếp nhận, xác định sự cố:

Đơn vị vận hành hệ thống thông tin chủ trì, phối hợp với Đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng tỉnh Hà Tĩnh và các cơ quan, tổ chức liên quan tiếp nhận, phân tích các cảnh báo, dấu hiệu sự cố từ các nguồn bên trong và bên ngoài (cảnh báo sự cố: Công văn, 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, 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...

1.2. Triển khai các bước ưu tiên ứng cứu ban đầu:

Sau khi đã xác định sự cố xảy ra, đơn vị vận hành hệ thống thông tin 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.

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.

1.3. Thông báo, báo cáo sự cố:

Sau khi triển khai các bước ưu tiên ứng cứu ban đầu, đơn vị vận hành hệ thống thông tin tổ chức thông báo, báo cáo sự cố đến các tổ chức, cá nhân liên quan bên trong và bên ngoài cơ quan, tổ chức theo quy định. Cụ thể:

- Thông báo sự cố tới cơ quan chủ quản Đội ứng cứu sự cố chậm nhất 3 ngày kể từ khi phát hiện sự cố; trường hợp xác định sự cố có thể vượt khả năng xử lý, đơn vị vận hành hệ thống thông tin phải báo cáo ban đầu sự cố bằng văn bản về Trung tâm CNTT và Truyền thông.
- Hình thức thông báo sự cố: Bằng công văn, fax, thư điện tử, nhắn tin đa phương tiện, phần mềm gửi nhận văn bản, phần mềm điều hành tác nghiệp, hoặc thông qua hệ thống kỹ thuật báo sự cố ATTT mạng của cơ quan điều phối cấp tỉnh.
- Hình thức báo cáo sự cố: Bằng văn bản giấy hoặc văn bản điện tử.

2. Ngăn chặn, xử lý sự cố

2.1. Chọn phương án:

Đơn vị vận hành hệ thống phối hợp với Đội ứng cứu sự cố và các đơn vị liên quan báo cáo, đề xuất cơ quan chủ quản hệ thống thông tin, Ban Chỉ đạo ứng cứu khẩn cấp sự cố an toàn thông tin mạng của tỉnh, 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.

Đơn vị vận hành hệ thống phối hợp với Đội ứng cứu sự cố, Trung tâm CNTT và Truyền thông và các đơn vị liên quan tiến hành:

- Phân loại sự cố:

+ Sự cố về tấn công từ chối dịch vụ;
+ Sự cố về tấn công giả mạo;
+ Sự cố về tấn công sử dụng mã độc;
+ Sự cố về tấn công truy cập trái phép, chiếm quyền điều khiển;
+ Sự cố về tấn công thay đổi giao diện;
+ Sự cố về tấn công mã hóa phần mềm, dữ liệu, thiết bị;
+ Sự cố về tấn công phá hoại thông tin, dữ liệu, phần mềm;
+ Sự cố về tấn công nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu;
+ Sự cố về tấn công tổng hợp sử dụng kết hợp nhiều hình thức;
+ Sự cố về các hình thức tấn công mạng khác.

- Báo cáo lãnh đạo đơn vị: Chỉ đạo xử lý và phân công trách nhiệm xử lý.
- Thu thập thông tin để phục vụ phân tích sự cố:

+ Thông tin về đầu mối liên hệ;
+ Thu thập thông tin hệ thống;
+ Thu thập chức năng của hệ thống;
+ Thu thập cấu hình của hệ thống (OS, Servise, version, network...);
+ Thu thập chứng cứ;
+ Thu thập bộ nhớ;
+ Thu thập trạng thái network và các kết nối;
+ Thu thập các tiến trình đang chạy;
+ Thu thập hard drive media;
+ Thu thập log file;
+ Thu thập các cổng đang mở của hệ thống.

- Phân tích sự cố:

+ Phân tích dòng thời gian;
+ Thời gian bị sửa đổi, truy cập, tạo hoặc thay đổi.
+ Thời gian thực hiện các cập nhật lớn đối với hệ thống;
+ Thời điểm mà hệ thống sử dụng lần cuối cùng;
+ Phân tích dữ liệu ...

- Xử lý sự cố:

+ Gỡ bỏ sự cố;
+ Xác định và gỡ bỏ các backdoors;
+ Phân tích và kiểm tra lỗ hổng sau khi thực hiện các bản vá lỗi;
+ Khôi phục;
+ Phân tích và kiểm tra lỗ hổng sau khi thực hiện các bản vá lỗi;
+ Khôi phục dữ liệu;
+ Thu thập các tệp tin, hình ảnh, email,... bị xóa, thời gian bị xóa;

+ Tìm kiếm các tệp tin không thể khôi phục;

+ Khôi phục các tệp tin phù hợp.

- Tổng hợp báo cáo Lãnh đạo đơn vị và Trung tâm CNTT và Truyền thông:

+ Báo cáo kết quả phân tích sự cố: Mô tả chi tiết các bước quan trọng khi thực hiện xử lý sự cố;

+ Tổng hợp báo cáo gửi lãnh đạo cơ quan, tổ chức và các bên liên quan đến sự cố;

+ Rút kinh nghiệm và ứng dụng cho các sự cố tương tự.

2.2. Triển khai thu thập chứng cứ:

Trên cơ sở phương án, nguồn lực đã được phê duyệt, đơn vị được giao hoặc Đội ứng cứu sự cố tổ chức thu thập chứng cứ, phạm vi, đối tượng bị ảnh hưởng,...

2.3. Xác định nguồn gốc tấn công:

Đơn vị được giao hoặc 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.

3. Khắc phục, gỡ bỏ và khôi phục

3.1. 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).

3.2. Khôi phục:

Đơn vị vận hành hệ thống 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.

Trong quá trình ứng cứu sự cố, đơn vị vận hành hệ thống phải chủ trì, phối hợp với các cơ quan, đơn vị liên quan xây dựng và duy trì thực hiện các báo cáo ứng cứu sự cố gồm:

+ Báo cáo ban đầu;

+ Báo cáo diễn biến tình hình;

+ Báo cáo phương án ứng cứu cụ thể;

+ Báo cáo xin ý kiến chỉ đạo, chỉ huy;

+ Báo cáo đề nghị hỗ trợ, phối hợp;

+ Báo cáo kết thúc ứng phó sự cố.

4. Tổng kết, đánh giá

4.1. Tổng kết, đúc rút kinh nghiệm:

Đơn vị vận hành hệ thống bị sự cố phối hợp với Đội ứng cứu sự cố và Trung tâm CNTT và Truyền thông triển khai tổng hợp tất cả các thông tin, báo cáo, phân tích có liên quan đến sự cố, công tác triển khai phương án ứng cứu khẩn cấp bảo đảm ATTT mạng, báo cáo Ban Chỉ đạo ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh; 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...

4.2. Xây dựng báo cáo kết thúc ứng cứu sự cố:

Đơn vị vận hành hệ thống thông tin bị sự cố, Đội ứng cứu sự cố, Trung tâm CNTT và Truyền thông chịu trách nhiệm chủ trì ứng cứu sự cố 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.

Sau khi kết thúc ứng cứu sự cố, trong vòng 10 ngày đơn vị vận hành hệ thống thông tin, đơn vị được giao chủ trì ứng cứu hệ thống thông tin bị sự cố phải xây dựng báo cáo kết thúc ứng phó sự cố, gửi về Đội ứng cứu sự cố, Trung tâm CNTT và Truyền thông.

- Cách thức thực hiện:

+ Nộp hồ sơ trực tiếp.

+ Nộp hồ sơ qua dịch vụ bưu chính.

+ Nộp hồ sơ qua phần mềm quản lý văn bản và hồ sơ công việc (https://hscv.hatinh.gov.vn).

+ Nộp hồ sơ qua Hệ thống thông tin giải quyết TTHC của tỉnh (https://dichvucong.hatinh.gov.vn)

- Thành phần, số lượng hồ sơ:

1. Văn bản đề nghị Ứng cứu xử lý sự cố an toàn thông tin của các hệ thống thông tin;

2. Tài liệu mô tả, thuyết minh tổng quan về hệ thống thông tin;

3. Hồ sơ đề xuất cấp độ đã được phê duyệt;

4. Hồ sơ thuyết minh phương án đảm bảo an toàn thông tin hệ thống.

- Thời hạn giải quyết: Không có quy định chính thức. Thực hiện theo tiến độ ứng cứu sự cố.

- Đối tượng thực hiện: Các cơ quan, tổ chức, đơn vị thuộc tỉnh.

- Cơ quan giải quyết:

- Cơ quan có thẩm quyền quyết định: UBND tỉnh.

- Cơ quan trực tiếp thực hiện TTHC: Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Hà Tĩnh.

- Cơ quan phối hợp thực hiện TTHC: Sở Thông tin và Truyền thông.

- Kết quả thực hiện thủ tục hành chính: Văn bản, thông báo khắc phục sự cố cho hệ thống thông tin

- Tên mẫu đơn, mẫu tờ khai: Văn bản mẫu số 03 ban hành kèm theo Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ trưởng Bộ Thông tin

và Truyền thông Quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc

- Yêu cầu, điều kiện thực hiện thủ tục hành chính: Không quy định.

- Căn cứ pháp lý của thủ tục hành chính:

1. Luật An toàn thông tin mạng ngày 19/11/2015;

2. 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;

3. Thông tư số 20/2017/TT-BTTTT ngày 01/11/2017 của Bộ Thông tin và Truyền thông Quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;

4. Quyết định số 01/2019/QĐ-UBND ngày 19/11/2019 của UBND tỉnh ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Hà Tĩnh;

5. Quyết định số 1111/QĐ-UBND ngày 31/5/2022 của UBND tỉnh về việc kiện toàn Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Hà Tĩnh.

BÁO CÁO BAN ĐẦU SỰ CỐ MẠNG

THÔNG TIN VỀ TỔ CHỨC/CÁ NHÂN BÁO CÁO SỰ CỐ

▪ Tên tổ chức/cá nhân báo cáo sự cố (*) .....

▪ Địa chỉ: (*) .....

▪ Điện thoại (*) ……Email (*) .....

NGƯỜI LIÊN HỆ

▪ Họ và tên (*) …… Chức vụ: .....

▪ Điện thoại (*) …… Email (*) .....

THÔNG TIN CHI TIẾT VỀ HỆ THỐNG BỊ SỰ CỐ

Tên đơn vị vận hành hệ thống thông tin (*):	*Điền tên đơn vị vận hành hoặc được thuê vận hành hệ thống thông tin*				
Cơ quan chủ quản:	*Điền tên cơ quan chủ quản*				
Tên hệ thống bị sự cố	*Điền tên hệ thống bị sự cố và tên miền, địa chỉ ip liên quan*				
Phân loại cấp độ của hệ thống thông tin (nếu có)	□ Cấp độ 1	□ Cấp độ 2	□ Cấp độ 3	□ Cấp độ 4	□ Cấp độ 5
Tổ chức cung cấp dịch vụ an toàn thông tin (nếu có):	*Điền tên nhà cung cấp ở đây*				
Tên nhà cung cấp dịch vụ kết nối bên ngoài (nếu có)	*Điền tên nhà cung cấp ở đây*				
Điền tên nhà cung cấp ở đây	*Điền thông tin ở đây*				

Mô tả sơ bộ về sự cố (*)
Đề nghị cung cấp một bản tóm tắt ngắn gọn về sự cố, bao gồm đánh giá sơ bộ cuộc tấn công đã xảy ra chưa và bất kỳ các nguy cơ dẫn đến khả năng phá hoại hoặc gián đoạn dịch vụ. Cũng vui lòng xác định mức độ nhạy cảm của thông tin liên quan hoặc những đối tượng bị ảnh hưởng bởi sự cố: ....

Ngày phát hiện sự cố (*) (dd/mm/yy)	/ /	Thời gian phát hiện (*):	…… giờ.... phút

HIỆN TRẠNG SỰ CỐ (*)

□ Đã được xử lý □ Chưa được xử lý

CÁCH THỨC PHÁT HIỆN

***** *(Đánh dấu những cách thức được sử dụng để phát hiện sự cố)*

□ Qua hệ thống phát hiện xâm nhập □ Kiểm tra dữ liệu lưu lại (Log File)

□ Nhận được thông báo từ: .....

□ Khác, đó là .....

ĐÃ GỬI THÔNG BÁO SỰ CỐ CHO *

□ Thành viên mạng lưới chịu trách nhiệm ứng cứu sự cố cho tổ chức, cá nhân

□ ISP đang trực tiếp cung cấp dịch vụ

□ Cơ quan điều phối

THÔNG TIN BỔ SUNG VỀ HỆ THỐNG XẢY RA SỰ CỐ

▪ Hệ điều hành ……Version .....

▪ Các dịch vụ có trên hệ thống *(Đánh dấu những dịch vụ được sử dụng trên hệ thống)*

□ Web server □ Mail server □ Database server

□ Dịch vụ khác, đó là .....

▪ Các biện pháp an toàn thông tin đã triển khai *(Đánh dấu những biện pháp đã triển khai)*

□ Antivirus □ Firewall □ Hệ thống phát hiện xâm nhập

□ Khác:

▪ Các địa chỉ IP của hệ thống *(Liệt kê địa chỉ IP sử dụng trên Internet, không liệt kê địa chỉ IP nội bộ)*

.....

▪ Các tên miền của hệ thống .....

▪ Mục đích chính sử dụng hệ thống .....

▪ Thông tin gửi kèm

□ Nhật ký hệ thống □ Mẫu virus / mã độc □ Khác:.....……..

▪ Các thông tin cung cấp trong thông báo sự cố này đều phải được giữ bí mật: □ Có □ Không

KIẾN NGHỊ, ĐỀ XUẤT HỖ TRỢ

Mô tả về đề xuất, kiến nghị
Đề nghị cung cấp tóm lược về các kiến nghị và đề xuất hỗ trợ ứng cứu (nếu có) ....

THỜI GIAN THỰC HIỆN BÁO CÁO SỰ CỐ

*: …/…/…../…(ngày/tháng/năm/giờ/phút)

CÁ NHÂN/NGƯỜI ĐẠI DIỆN THEO PHÁP LUẬT
(Ký tên, đóng dấu)

Chú thích: 1. Phần (*) là những thông tin bắt buộc. Các phần còn lại có thể loại bỏ nếu không có thông tin.

2. Sử dụng tiêu đề (subject) bắt đầu bằng ‘‘[TBSC]” khi gửi thông báo qua email

3. Tham khảo thêm tại website của VNCERT (www.vncert.gov vn)