ỦY BAN NHÂN DÂN TỈNH THANH HÓA	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 2777 /QĐ-UBND	*Thanh Hóa, ngày 29 tháng 8 năm 2026*

QUYẾT ĐỊNH
Về việc ban hành Phương án ứng cứu sự cố, bảo đảm an toàn, an ninh mạng trên địa bàn tỉnh Thanh Hóa

ỦY BAN NHÂN DÂN TỈNH THANH HÓA

Căn cứ Luật Tổ chức chính quyền địa phương số 72/2025/QH15 ngày 16 tháng 6 năm 2025;

Căn cứ Luật Giao dịch điện tử số 20/2023/QH15 ngày 22 tháng 6 năm 2023; Luật Viễn thông số 24/2023/QH15 ngày 24 tháng 11 năm 2023;

Căn cứ Luật Dữ liệu số 60/2024/QH15 ngày 30 tháng 11 năm 2024; Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 ngày 26 tháng 6 năm 2025;

Căn cứ Luật An ninh mạng số 116/2025/QH15 ngày 10 tháng 12 năm 2025; Luật Bảo vệ bí mật nhà nước số 117/2025/QH15 ngày 10 tháng 12 năm 2025; Luật Chuyển đổi số số 148/2025/QH15 ngày 11 tháng 12 năm 2025;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ; Nghị định số 165/2025/NĐ-CP ngày 30 tháng 6 năm 2025 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Dữ liệu;

Căn cứ Nghị định số 356/2025/NĐ-CP ngày 31 tháng 12 năm 2025 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Bảo vệ dữ liệu cá nhân; Nghị định số 63/2026/NĐ-CP ngày 28 tháng 02 năm 2026 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Bảo vệ bí mật nhà nước; Nghị định số 224/2026/NĐ-CP ngày 24 tháng 6 năm 2026 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Chuyển đổi số;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 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; Quyết định số 964/QĐ-TTg ngày 10 tháng 8 năm 2022 của Thủ tướng Chính phủ phê duyệt Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn đến năm 2030; Quyết định số 437/QĐ-TTg ngày 16 tháng 3 năm 2026 của Thủ tướng Chính phủ ban hành Kế hoạch triển khai thi hành Luật An ninh mạng;

Căn cứ Chỉ thị số 18/CT-TTg ngày 13 tháng 10 năm 2022 của Thủ tướng Chính phủ về đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin

mạng Việt Nam; Chỉ thị số 23/CT-TTg ngày 26 tháng 12 năm 2022 về tăng cường công tác bảo đảm an ninh, an toàn thông tin cho thiết bị camera giám sát; Chỉ thị số 09/CT-TTg ngày 23 tháng 02 năm 2024 về tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 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; Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP;

Căn cứ Quyết định số 44/2025/QĐ-UBND ngày 16 tháng 5 năm 2025 của UBND tỉnh Thanh Hóa ban hành Quy chế quản lý, vận hành, kết nối, bảo đảm an toàn thông tin và sử dụng mạng truyền số liệu chuyên dùng trên địa bàn tỉnh Thanh Hóa;

Thực hiện Kế hoạch số 150/KH-UBND ngày 19 tháng 5 năm 2026 của UBND tỉnh Thanh Hóa về ứng cứu sự cố, bảo đảm an toàn, an ninh mạng trên địa bàn tỉnh Thanh Hóa;

Theo đề nghị của Giám đốc Công an tỉnh tại Tờ trình số 376/TTr-CAT-ANM&PCTPSDCNC ngày 22 tháng 8 năm 2026.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Phương án ứng cứu sự cố, bảo đảm an toàn, an ninh mạng trên địa bàn tỉnh Thanh Hóa.

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

Điều 3. Chánh Văn phòng Ủy ban nhân dân tỉnh; Giám đốc Công an tỉnh; Thủ trưởng các sở, ban, ngành, đơn vị, đoàn thể cấp tỉnh; Chủ tịch UBND các xã, phường và các tổ chức, cá nhân liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Bộ Công an
- Thường trực :Tỉnh ủy, HĐND tỉnh (để b/c);
- Chủ tịch UBND tỉnh
- Các PCT UBND tỉnh;
- Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Bộ Công an (để p/h);
- Ủy ban MTTQ Việt Nam tỉnh;
- Công an tỉnh;
- Các sở, ban, ngành, đơn vị, đoàn thể cấp tỉnh;
- Đảng ủy, UBND các xã, phường;
- Lưu: VT, NNMT, TDNC.

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

Cao Văn Cường

ỦY BAN NHÂN DÂN **TỈNH THANH HÓA**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**

PHƯƠNG ÁN

Ứng cứu sự cố, bảo đảm an toàn, an ninh mạng trên địa bàn tỉnh Thanh Hóa

(kèm theo Quyết định số /QĐ-UBND ngày / /2026 của UBND tỉnh Thanh Hóa)

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Thiết lập cơ chế thống nhất, đồng bộ để phát hiện, tiếp nhận báo cáo, chỉ đạo, huy động lực lượng, phối hợp ứng cứu, khắc phục và xử lý hậu quả khi xảy ra sự cố an ninh mạng trên địa bàn tỉnh; bảo đảm sự liên thông giữa lực lượng tại chỗ, lực lượng cấp tỉnh và cơ quan, đơn vị Trung ương khi cần thiết.

- Bảo đảm duy trì liên tục, an toàn hoạt động chỉ đạo, điều hành của các cơ quan trong hệ thống chính trị; việc cung cấp dịch vụ công, giải quyết thủ tục hành chính; vận hành cơ sở dữ liệu, nền tảng số dùng chung, hệ thống thông tin chuyên ngành và dịch vụ thiết yếu; hạn chế thấp nhất thiệt hại, thời gian gián đoạn, phạm vi lây lan và tác động tiêu cực đối với người dân, doanh nghiệp, cơ quan, tổ chức.

- Xác định rõ thẩm quyền quyết định, trách nhiệm của người Chỉ đạo chung, cơ quan thường trực, Đội trưởng đội ứng cứu sự cố an ninh mạng, Đội ứng cứu sự cố, cơ quan chủ quản, đơn vị vận hành, bộ phận hoặc đầu mối tại chỗ; phân định cụ thể đơn vị chủ trì, đơn vị phối hợp đối với từng mức độ sự cố, từng giai đoạn xử lý và từng nhóm hệ thống thông tin, không để chồng chéo, bỏ trống nhiệm vụ hoặc chậm trễ trong tổ chức thực hiện.

- Bảo đảm hoạt động ứng cứu sự cố gắn với bảo vệ dữ liệu cá nhân, dữ liệu quan trọng, dữ liệu cốt lõi, bí mật nhà nước, hồ sơ điện tử; quản lý, bảo toàn dữ liệu điện tử, tài liệu, thiết bị và nhật ký hệ thống phục vụ xác minh, điều tra; thực hiện đầy đủ nghĩa vụ báo cáo, thông báo, xử lý vi phạm và áp dụng biện pháp phòng ngừa sự cố tái diễn theo quy định của pháp luật.

- Làm căn cứ để các sở, ban, ngành, đơn vị cấp tỉnh, Ủy ban nhân dân các xã, phường, cơ quan chủ quản, đơn vị vận hành và doanh nghiệp có liên quan xây dựng hoặc cập nhật phương án ứng cứu sự cố nội bộ; bố trí đầu mối thường trực, nhân lực, trang thiết bị, công cụ, kinh phí, phương án sao lưu, dự phòng, khôi phục và hợp đồng hỗ trợ kỹ thuật phù hợp với từng hệ thống thông tin.

- Nâng cao năng lực tổ chức, phối hợp và khả năng phản ứng của Đội ứng

cứu sự cố an ninh mạng tỉnh Thanh Hóa và lực lượng tại các cơ quan, đơn vị; tạo cơ sở để tổ chức tập huấn, diễn tập, kiểm tra, đánh giá, chia sẻ cảnh báo và thường xuyên hoàn thiện quy trình, kịch bản ứng cứu phù hợp với tình hình thực tế.

2. Yêu cầu

- Việc ứng cứu sự cố trước hết phải được tổ chức bằng lực lượng tại chỗ. Đơn vị vận hành hệ thống thông tin trực tiếp thực hiện biện pháp xử lý an toàn ban đầu; cơ quan chủ quản chịu trách nhiệm đối với hệ thống, dữ liệu và dịch vụ thuộc phạm vi quản lý; đồng thời phải báo cáo ngay, phối hợp chặt chẽ với Công an tỉnh, Cơ quan thường trực và Đội ứng cứu sự cố theo quy định.

- Bảo đảm sự Chỉ đạo tập trung, thống nhất; duy trì một đầu mối điều phối, một chế độ báo cáo và một nguồn thông tin chính thức. Mọi yêu cầu huy động lực lượng, thay đổi cấu hình, tạm dừng dịch vụ, chuyển sang hệ thống dự phòng hoặc cung cấp thông tin công khai phải được thực hiện đúng thẩm quyền và được ghi nhận đầy đủ.

- Tổ chức xử lý nhanh chóng, kịp thời, chính xác nhưng không làm mất, thay đổi hoặc phá hủy dữ liệu điện tử, tài liệu, thiết bị và nhật ký hệ thống phục vụ xác minh, điều tra; không làm mở rộng phạm vi lây nhiễm, không tự ý xóa dữ liệu, cài đặt lại hoặc đưa hệ thống chưa được kiểm tra an toàn trở lại hoạt động.

- Đánh giá, phân loại sự cố trên cơ sở phạm vi ảnh hưởng, mức độ gián đoạn dịch vụ, nguy cơ đối với dữ liệu, tính chất hành vi và khả năng xử lý của cơ quan, đơn vị; khi chưa xác định đầy đủ phạm vi hoặc có dấu hiệu tấn công có chủ đích phải áp dụng cơ chế huy động lực lượng ở mức cao hơn để chủ động kiểm soát và kịp thời báo cáo người có thẩm quyền.

- Ưu tiên bảo vệ tính mạng, sức khỏe con người, môi trường; duy trì hoạt động chỉ đạo, điều hành, thông tin liên lạc, dịch vụ thiết yếu, dịch vụ công và dữ liệu không thể tái tạo; thực hiện phương án nghiệp vụ thay thế hoặc vận hành thủ công trong suốt thời gian hệ thống bị gián đoạn.

- Mọi thao tác cô lập, thay đổi cấu hình, thu thập, sao chép, bàn giao, khôi phục, kiểm thử và kết nối trở lại phải xác định rõ người thực hiện, thời gian, nội dung, căn cứ, người phê duyệt và kết quả; bảo đảm khả năng kiểm tra, đối chiếu và xác định trách nhiệm sau sự cố.

- Bảo đảm sẵn sàng đầu mối tiếp nhận thông tin 24 giờ trong ngày, 07 ngày trong tuần; bảo đảm điều kiện về nhân lực, trang thiết bị, công cụ, phần mềm có bản quyền, bản sao lưu, hệ thống dự phòng, hợp đồng hỗ trợ và kinh phí cần thiết; thường xuyên kiểm tra khả năng khôi phục, tổ chức tập huấn, diễn tập và cập nhật Phương án.

- Việc triển khai Phương án phải tuân thủ quy định của pháp luật về an ninh

mạng, dữ liệu, bảo vệ dữ liệu cá nhân, bảo vệ bí mật nhà nước, phòng cháy, chữa cháy, phòng chống thiên tai và các quy định chuyên ngành; bảo đảm thống nhất với Kế hoạch số 150/KH-UBND và các phương án, quy trình đã được cấp có thẩm quyền ban hành.

3. Phạm vi và đối tượng áp dụng

Phương án áp dụng đối với hệ thống thông tin, nền tảng số, cơ sở dữ liệu, tài nguyên số, mạng truyền số liệu chuyên dùng, hạ tầng viễn thông - công nghệ thông tin, trung tâm dữ liệu, dịch vụ điện toán đám mây, thiết bị đầu cuối, hệ thống camera sử dụng giao thức Internet, thiết bị kết nối Internet vạn vật, hệ thống điều khiển giám sát và thu thập dữ liệu, hệ thống điều khiển công nghiệp thuộc phạm vi quản lý của tỉnh hoặc cung cấp dịch vụ, kết nối, chia sẻ dữ liệu cho cơ quan, đơn vị trên địa bàn tỉnh.

Đối tượng áp dụng gồm: các sở, ban, ngành, đơn vị, đoàn thể cấp tỉnh; UBND các xã, phường; đơn vị sự nghiệp, doanh nghiệp nhà nước thuộc tỉnh; cơ quan chủ quản hệ thống thông tin, đơn vị vận hành hệ thống thông tin; Đội ứng cứu sự cố an ninh mạng tỉnh Thanh Hóa (sau đây gọi tắt là Đội ứng cứu sự cố); bộ phận hoặc đầu mối ứng cứu sự cố tại chỗ; doanh nghiệp viễn thông, điện lực, cấp nước, điện toán đám mây, công nghệ, an ninh mạng và tổ chức, cá nhân có liên quan.

Đối với hệ thống thuộc Công an, Quân đội, cơ yếu hoặc hệ thống có phương án chuyên ngành, phương án mật riêng thì thực hiện theo quy định chuyên ngành; Phương án này được vận dụng để phối hợp các nguồn lực của tỉnh khi có yêu cầu hợp pháp của cơ quan có thẩm quyền.

4. Nguyên tắc áp dụng

- Tập trung ứng cứu sự cố tại chỗ là chính, phối hợp kịp thời cấp có thẩm quyền thuộc Trung ương và địa phương khi vượt khả năng hoặc thẩm quyền.

- Cơ quan chủ quản chịu trách nhiệm cuối cùng về duy trì, tạm dừng, chuyển dự phòng, khôi phục và đưa hệ thống trở lại hoạt động; Công an tỉnh điều phối chuyên môn an ninh mạng và thực hiện chức năng điều tra, xử lý theo thẩm quyền.

- Không chờ xác định đầy đủ nguyên nhân, đối tượng hoặc thiệt hại mới báo cáo; báo cáo ban đầu có thể chưa hoàn chỉnh nhưng phải đúng hiện trạng đã biết và được cập nhật liên tục.

- Cô lập có kiểm soát, ưu tiên chặn đường lây lan, tài khoản đặc quyền và kênh truy cập từ xa; không tự ý tắt nguồn, khởi động lại, cài lại hệ điều hành hoặc xóa dữ liệu khi có dấu hiệu tấn công.

- Bảo toàn bí mật nhà nước, dữ liệu cá nhân và dữ liệu điện tử quan trọng, tài liệu, thiết bị phục vụ xác minh, điều tra; chia sẻ thông tin theo nguyên tắc cần biết, đúng thẩm quyền, có ghi nhận và kênh bảo mật.

- Không tự ý liên hệ, đàm phán và tự xử lý đối với đối tượng tấn công; không đưa thông tin chưa được kiểm chứng lên báo chí, mạng xã hội hoặc kênh trao đổi không được phép.

- Phương án chuyên ngành về phòng cháy, chữa cháy, phòng chống thiên tai, an toàn điện, an toàn vận hành công nghiệp, y tế và giao thông được thực hiện đồng thời; ưu tiên tuyệt đối an toàn con người và môi trường.

- Các thuật ngữ, chữ viết tắt chuyên ngành chỉ được sử dụng sau khi đã viết đầy đủ và giải nghĩa tại lần xuất hiện đầu tiên; ưu tiên sử dụng thuật ngữ tiếng Việt trong văn bản, báo cáo và trao đổi điều phối.

5. Giải thích từ ngữ và chữ viết tắt

a) Trong nội dung Phương án này, các từ ngữ dưới đây được hiểu như sau:

- "*Sự cố an ninh mạng*" là tình huống, sự việc bất ngờ xảy ra đối với thông tin, dữ liệu hoặc hệ thống thông tin trên không gian mạng, làm ảnh hưởng hoặc có nguy cơ làm ảnh hưởng đến tính bí mật, tính toàn vẹn, tính sẵn sàng của thông tin, dữ liệu, hoạt động bình thường của hệ thống thông tin, có nguy cơ xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

- "*Ứng cứu sự cố*" là tổng hợp các hoạt động tiếp nhận, xác minh, đánh giá, phân loại, báo cáo, huy động lực lượng, ngăn chặn, xử lý nguyên nhân, khắc phục hậu quả, khôi phục hệ thống, giám sát sau khôi phục và các hoạt động có liên quan nhằm hạn chế thiệt hại, đưa hệ thống trở lại hoạt động an toàn.

- "*Cơ quan chủ quản hệ thống thông tin*" là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin.

- "*Đơn vị vận hành hệ thống thông tin*" là cơ quan, tổ chức, doanh nghiệp trực tiếp quản trị, vận hành hệ thống thông tin theo phân công của cơ quan chủ quản hoặc theo hợp đồng cung cấp dịch vụ.

- "*Đội ứng cứu sự cố*" là Đội ứng cứu sự cố an ninh mạng tỉnh Thanh Hóa được thành lập theo Quyết định của Chủ tịch Ủy ban nhân dân tỉnh; Công an tỉnh là Cơ quan thường trực của Đội ứng cứu sự cố, Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao là bộ phận giúp việc, thường trực.

- "*Bộ phận hoặc đầu mối ứng cứu sự cố tại chỗ*" là bộ phận, tổ hoặc cá nhân được người đứng đầu cơ quan, đơn vị giao nhiệm vụ tiếp nhận cảnh báo, thực hiện biện pháp xử lý ban đầu, báo cáo và phối hợp với Công an tỉnh, Đội ứng cứu sự cố trong quá trình xử lý.

- Trong khuôn khổ Phương án này, Mức 1, Mức 2, Mức 3 là các mức huy động lực lượng ứng cứu, được xác định căn cứ tính chất, phạm vi ảnh hưởng, khả năng kiểm soát, xử lý của cơ quan chủ quản, đơn vị vận hành và yêu cầu phối hợp

các lực lượng có liên quan; không thay thế việc phân loại sự cố theo quy định của pháp luật. Cụ thể như sau:

+ Mức 1: Ứng cứu sự cố tại chỗ, cơ quan chủ quản, đơn vị vận hành và lực lượng tại chỗ có khả năng kiểm soát, xử lý sự cố;

+ Mức 2: Huy động phối hợp cấp tỉnh khi sự cố vượt quá hoặc có nguy cơ vượt khả năng xử lý tại chỗ; Công an tỉnh, với tư cách Cơ quan thường trực của Đội ứng cứu sự cố, tham mưu huy động Đội ứng cứu sự cố an ninh mạng tỉnh và các cơ quan, đơn vị, doanh nghiệp có liên quan tham gia phối hợp theo chức năng, nhiệm vụ.

+ Mức 3: Huy động khẩn cấp, diện rộng khi sự cố nghiêm trọng theo quy định của pháp luật hoặc có dấu hiệu, nguy cơ gây hậu quả nghiêm trọng, cần sự chỉ đạo, điều phối và huy động nguồn lực ở phạm vi cấp tỉnh hoặc đề nghị cơ quan Trung ương hỗ trợ.

Việc phân mức nêu trên chỉ phục vụ tổ chức chỉ đạo, điều phối và huy động lực lượng trong phạm vi Phương án này; không thay thế việc phân nhóm sự cố thông thường, sự cố nghiêm trọng theo Quyết định số 05/2017/QĐ-TTg, không thay thế việc xác định cấp độ hệ thống thông tin theo quy định của pháp luật.

Trường hợp đánh giá sự cố an ninh mạng là nghiêm trọng theo Quyết định số 05/2017/QĐ-TTg thì thực hiện đầy đủ quy trình ứng cứu sự cố nghiêm trọng theo Điều 14 Quyết định này và các quy định có liên quan; đồng thời thực hiện tổ chức, huy động lực lượng ứng cứu sự cố theo Mức 3 của Phương án này.

II. ĐÁNH GIÁ NGUY CƠ, HỆ THỐNG TRỌNG ĐIỂM VÀ GIẢ ĐỊNH PHỤC VỤ TRIỂN KHAI ỨNG CỨU

1. Đặc điểm và quan hệ phụ thuộc cần tính đến khi thực hiện ứng cứu

- Các hệ thống dùng chung của tỉnh tập trung tại Trung tâm dữ liệu, kết nối qua mạng truyền số liệu chuyên dùng, mạng Internet và nền tảng tích hợp, chia sẻ dữ liệu; sự cố tại hạ tầng định danh, dịch vụ phân giải tên miền, nền tảng ảo hóa, lưu trữ, cơ sở dữ liệu hoặc đường truyền có thể gây ảnh hưởng đồng thời đến nhiều dịch vụ.

- Các sở, ngành và UBND xã, phường sử dụng kết hợp hệ thống tập trung, hệ thống chuyên ngành của bộ, ngành, dịch vụ điện toán đám mây và sản phẩm do các tổ chức, cá nhân liên quan vận hành; trách nhiệm ứng cứu phải bao quát cả trách nhiệm, nghĩa vụ khi thực hiện các nội dung trong hợp đồng ký kết từ các tổ chức, cá nhân liên quan đến lắp đặt, vận hành, bảo trì.

- Nhiều hệ thống xử lý dữ liệu cá nhân, hồ sơ điện tử, dữ liệu chuyên ngành, bí mật nhà nước và dữ liệu không thể tái tạo; việc khôi phục nhanh phải đi kèm đối soát tính toàn vẹn, nguồn gốc và thẩm quyền truy cập.

- Các hệ thống điện, nước, y tế, giao thông, công nghiệp và quan trắc có thể gắn với thiết bị vật lý, hệ thống điều khiển giám sát, thu thập dữ liệu và hệ thống điều khiển công nghiệp; việc thực hiện biện pháp kỹ thuật phải tuân thủ quy trình an toàn vận hành và an toàn vật lý của đơn vị chuyên ngành.

2. Nhóm hệ thống, dữ liệu và dịch vụ ưu tiên bảo vệ, khôi phục

Các hệ thống thông tin, dữ liệu và dịch vụ cần ưu tiên xem xét bảo vệ, duy trì và khôi phục trên địa bàn tỉnh gồm:

a) Hệ thống thông tin chỉ đạo, điều hành và thông tin khẩn cấp

Hệ thống quản lý văn bản, thư điện tử công vụ, hội nghị trực tuyến, kênh chỉ đạo điều hành, thông tin phục vụ lãnh đạo tỉnh.

b) Hạ tầng nền tảng dùng chung

Trung tâm dữ liệu; mạng truyền số liệu chuyên dùng; hạ tầng định danh, phân giải tên miền và đồng bộ thời gian; nền tảng ảo hóa, lưu trữ, sao lưu; hệ thống giám sát an ninh mạng, giám sát vận hành mạng và Trung tâm Điều hành thông minh.

c) Hệ thống thông tin cung cấp dịch vụ công và thủ tục hành chính

Hệ thống thông tin giải quyết thủ tục hành chính; Cổng Dịch vụ công; thanh toán, ký số, tiếp nhận và trả kết quả.

d) Hệ thống thông tin lưu trữ, xử lý cơ sở dữ liệu quan trọng

Đất đai, tài chính - ngân sách, hộ tịch, cán bộ, y tế, giáo dục và cơ sở dữ liệu chuyên ngành.

đ) Hệ thống thông tin cung cấp dịch vụ thiết yếu hoặc vận hành hệ thống công nghiệp

Điện lực, cấp nước, y tế cấp cứu, giao thông, khu công nghiệp, môi trường, hệ thống điều khiển giám sát, thu thập dữ liệu và hệ thống điều khiển công nghiệp.

e) Hệ thống thông tin tích hợp, chia sẻ dữ liệu

Nền tảng tích hợp, chia sẻ dữ liệu cấp tỉnh; cổng giao tiếp lập trình ứng dụng; trục kết nối, kho dữ liệu, nền tảng chia sẻ và đồng bộ dữ liệu.

g) Hệ thống thông tin công cộng và phục vụ hoạt động giám sát, bảo đảm an ninh trật tự

Cổng, trang thông tin điện tử; hệ thống camera, thiết bị ghi hình mạng; nền tảng cảnh báo, phản ánh, truyền thanh và thông tin cơ sở.

Trong đó, thứ tự ưu tiên ứng cứu sự cố không xác định cố định theo nhóm hệ thống nêu trên mà được người có thẩm quyền quyết định đối tình huống, sự cố an ninh mạng trên cơ sở mức độ quan trọng của hệ thống thông tin, thành phần

chức năng, ứng dụng, dịch vụ, dữ liệu cần bảo vệ; mức độ ảnh hưởng đến hoạt động chỉ đạo, điều hành, quyền và lợi ích hợp pháp của tổ chức, cá nhân, việc cung cấp dịch vụ công, dịch vụ thiết yếu; quan hệ phụ thuộc giữa các hệ thống và khả năng ứng cứu, khắc phục sự cố.

3. Nguy cơ và tình huống giả định chính

- Tấn công có chủ đích, khai thác lỗ hổng chưa công bố, chiếm tài khoản đặc quyền, di chuyển ngang và duy trì truy cập dài ngày.

- Mã độc tống tiền, mã độc phá hoại, mạng máy tính bị điều khiển trái phép, tấn công từ chối dịch vụ, thay đổi trái phép giao diện, giả mạo và lừa đảo trên diện rộng.

- Lộ lọt, sửa đổi, xóa hoặc gian lận dữ liệu do xâm nhập, cấu hình sai, lỗi người dùng, từ đội ngũ nhân sự vận hành, phía tổ chức, cá nhân cung cấp dịch vụ hoặc có các cá nhân xâm nhập trái phép từ bên trong để thực hiện hành vi tấn công mạng.

- Sự cố chuỗi cung ứng, bản cập nhật, thư viện, tài khoản hỗ trợ, dịch vụ đám mây hoặc nhà cung cấp bị xâm nhập.

- Gián đoạn nguồn điện, điều hòa, đường truyền, thiết bị lưu trữ, sao lưu, khóa mã hóa, cháy, ngập, thiên tai hoặc lỗi vận hành.

- Tấn công hệ thống camera, thiết bị kết nối Internet vạn vật hoặc mạng công nghệ vận hành; giả mạo tín hiệu, dữ liệu cảm biến hoặc lệnh điều khiển.

- Sự cố xảy ra ngoài giờ, đồng thời tại nhiều cơ quan, trong thời gian phục vụ sự kiện chính trị quan trọng hoặc khi kênh liên lạc chính bị gián đoạn.

4. Thứ tự ưu tiên khi tổ chức ứng cứu và khôi phục

Thứ tự ưu tiên chung là: (1) Bảo vệ tính mạng, an toàn con người và hiện trường; (2) duy trì chỉ đạo, liên lạc và kênh báo cáo; (3) ngăn chặn lây lan, bảo vệ tài khoản đặc quyền, hạ tầng định danh, mạng quản trị, vùng sao lưu và dữ liệu điện tử, tài liệu, thiết bị phục vụ xác minh, điều tra; (4) duy trì dịch vụ thiết yếu và dịch vụ công bằng phương án dự phòng hoặc phương thức thủ công; (5) khôi phục hạ tầng nền tảng, cơ sở dữ liệu và ứng dụng; (6) khôi phục các dịch vụ còn lại và thực hiện biện pháp khắc phục lâu dài.

5. Giả định phục vụ triển khai ứng cứu

- Danh mục hệ thống, sơ đồ mạng, tài khoản và hợp đồng được quản lý tại từng cơ quan chủ quản; thông tin nhạy cảm không đưa đầy đủ vào bản Phương án công khai.

- Mỗi cơ quan, đơn vị có ít nhất một đầu mối lãnh đạo, một đầu mối kỹ thuật và một đầu mối thay thế; danh sách được kiểm tra định kỳ và cung cấp cho Công an tỉnh.

- Trong trường hợp kênh điện tử không an toàn hoặc không khả dụng, sử dụng điện thoại, văn bản hỏa tốc, liên lạc trực tiếp hoặc kênh bảo mật khác do Công an tỉnh hướng dẫn.

III. TỔ CHỨC LỰC LƯỢNG, CƠ CHẾ CHỈ ĐẠO, ĐIỀU PHỐI VÀ THÔNG TIN LIÊN LẠC

1. Mô hình tổ chức lực lượng

Lực lượng ứng cứu sự cố được tổ chức theo nguyên tắc chỉ đạo thống nhất, phát huy trách nhiệm của cơ quan chủ quản và đơn vị vận hành, đồng thời huy động lực lượng cấp tỉnh theo tính chất, phạm vi và mức độ ảnh hưởng của sự cố. Thành phần trực tiếp gồm cơ quan chủ quản hệ thống thông tin, đơn vị vận hành hệ thống thông tin, bộ phận hoặc đầu mối ứng cứu sự cố tại chỗ, Công an tỉnh - Cơ quan thường trực của Đội ứng cứu sự cố và Đội ứng cứu sự cố; các sở, ban, ngành, địa phương, doanh nghiệp, tổ chức có liên quan và cơ quan Trung ương được huy động khi cần thiết.

a) Mức 1 - Xử lý tại chỗ

- Chỉ đạo chung: Người đứng đầu cơ quan chủ quản hoặc người được ủy quyền.

- Cơ quan, đơn vị chủ trì và điều phối: Đơn vị vận hành và bộ phận hoặc đầu mối ứng cứu sự cố tại chỗ

- Lực lượng phối hợp: Công an tỉnh tiếp nhận báo cáo, hướng dẫn, theo dõi và hỗ trợ khi có yêu cầu.

b) Mức 2 - Phối hợp cấp tỉnh

- Chỉ đạo chung: Lãnh đạo cơ quan chủ quản Chỉ đạo tại chỗ.

- Cơ quan, đơn vị chủ trì và điều phối: Cơ quan chủ quản Chỉ đạo tại chỗ; Công an tỉnh, với tư cách Cơ quan thường trực, tham mưu Đội trưởng đội ứng cứu sự cố an ninh mạng huy động Đội ứng cứu sự cố và tổ chức điều phối chuyên môn.

- Lực lượng phối hợp: Đội ứng cứu sự cố; Sở Khoa học và Công nghệ; sở, ngành chuyên môn; doanh nghiệp cung cấp dịch vụ.

c) Mức 3 - Khẩn cấp, diện rộng

- Chỉ đạo chung: Chủ tịch hoặc Phó Chủ tịch UBND tỉnh được phân công chỉ đạo chung.

- Cơ quan, đơn vị chủ trì và điều phối: Công an tỉnh tham mưu UBND tỉnh chỉ đạo chung; Đội trưởng đội ứng cứu sự cố an ninh mạng tổ chức lực lượng của Đội ứng cứu sự cố; cơ quan chủ quản hệ thống thông tin Chỉ đạo tại chỗ.

- Lực lượng phối hợp: Cơ quan chuyên trách thuộc Bộ Công an, cơ quan điều phối quốc gia, bộ, ngành, địa phương, doanh nghiệp và lực lượng liên quan.

2. Bộ phận Chỉ đạo và các vị trí chịu trách nhiệm

a) Chỉ đạo chung

Người chỉ đạo chung quyết định mục tiêu ưu tiên, mức độ huy động lực lượng, phạm vi tạm dừng dịch vụ, việc chuyển sang hệ thống dự phòng, sử dụng nguồn lực trong tình huống khẩn cấp, chế độ báo cáo và phương án cung cấp thông tin. Đối với sự cố Mức 3, Chủ tịch UBND tỉnh hoặc Phó Chủ tịch UBND tỉnh được phân công thực hiện chỉ đạo chung; đối với sự cố mức 1 và mức 2, người đứng đầu cơ quan chủ quản hệ thống thông tin chịu trách nhiệm Chỉ đạo tại chỗ trong phạm vi quản lý.

b) Cơ quan thường trực, điều phối

Công an tỉnh là Cơ quan thường trực của Đội ứng cứu sự cố; Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao là bộ phận giúp việc, thường trực của Đội. Công an tỉnh có trách nhiệm tiếp nhận, xác minh, đánh giá, phân loại sự cố; tham mưu Đội trưởng đội ứng cứu sự cố an ninh mạng huy động, phân công lực lượng; tổ chức điều phối chuyên môn theo chức năng, nhiệm vụ; hướng dẫn bảo toàn dữ liệu, tài liệu, thiết bị phục vụ xác minh, điều tra; tổng hợp, báo cáo UBND tỉnh và cơ quan cấp trên.

c) Chỉ đạo tại chỗ

Là lãnh đạo cơ quan chủ quản hệ thống thông tin hoặc người được ủy quyền; chịu trách nhiệm huy động nhân lực, cung cấp điều kiện tiếp cận; quyết định việc duy trì, tạm dừng hoặc chuyển sang hệ thống dự phòng; bảo vệ dữ liệu và người sử dụng; phối hợp cung cấp thông tin; phê duyệt khôi phục và chịu trách nhiệm tổ chức thực hiện kế hoạch khắc phục sau sự cố.

d) Chỉ đạo kỹ thuật

Là lãnh đạo đơn vị vận hành hệ thống thông tin hoặc người phụ trách kỹ thuật được cơ quan chủ quản giao nhiệm vụ; tổ chức thực hiện các biện pháp kỹ thuật theo phương án đã được thống nhất, kiểm soát thay đổi, phân công nhân sự, cập nhật diễn biến và quản lý nhật ký xử lý sự cố.

3. Đội ứng cứu sự cố và Cơ quan thường trực

- Đội trưởng đội ứng cứu sự cố an ninh mạng chịu trách nhiệm trước Chủ tịch UBND tỉnh về toàn bộ hoạt động của Đội; tổ chức phân công nhiệm vụ, quyết định phạm vi huy động thành viên đối với từng vụ việc và chỉ đạo hoạt động của Đội theo quy định của pháp luật, Quyết định thành lập Đội và Phương án này.

- Công an tỉnh là Cơ quan thường trực; Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao là bộ phận giúp việc, thường trực, có trách nhiệm tham mưu Đội trưởng đội ứng cứu sự cố an ninh mạng tổ chức hoạt động, tiếp nhận thông tin, chuẩn bị phương án huy động, tổng hợp kết quả và bảo đảm các

điều kiện cần thiết theo phân công. Việc sử dụng bộ máy, phương tiện, trang thiết bị và con dấu của Công an tỉnh để thực hiện nhiệm vụ của Đội được thực hiện theo Quyết định thành lập Đội, Quy chế hoạt động và quy định của pháp luật.

- Đội ứng cứu sự cố có nhiệm vụ hỗ trợ các sở, ban, ngành, đơn vị cấp tỉnh và UBND các xã, phường trong bảo đảm an ninh mạng; nghiên cứu, thu thập, xác minh, đánh giá, cảnh báo nguy cơ, sự cố và phần mềm độc hại; triển khai hoặc tham gia ứng cứu, phân tích, khắc phục, phục hồi hoạt động của hệ thống thông tin theo Quyết định số 05/2017/QĐ-TTg, Thông tư số 20/2017/TT-BTTTT, Kế hoạch số 150/KH-UBND, Quyết định thành lập Đội, Quy chế hoạt động và Phương án này; phối hợp với các lực lượng ứng cứu khác theo sự điều phối của cơ quan có thẩm quyền.

- Khi được huy động, thành viên Đội thực hiện nhiệm vụ theo phân công của Đội trưởng đội ứng cứu sự cố an ninh mạng, chịu sự điều phối của Cơ quan thường trực và phối hợp với Chỉ đạo tại chỗ; thủ trưởng cơ quan, đơn vị quản lý thành viên có trách nhiệm ưu tiên bố trí thời gian, phương tiện và điều kiện cần thiết để thành viên tham gia.

- Hoạt động nghiên cứu, xác minh, phân tích kỹ thuật của Đội không thay thế thẩm quyền điều tra, xử lý vi phạm của Công an tỉnh hoặc cơ quan có thẩm quyền; không thay thế trách nhiệm của cơ quan chủ quản và đơn vị vận hành đối với hệ thống thông tin.

- Hằng năm, Cơ quan thường trực tham mưu Đội trưởng đội ứng cứu sự cố an ninh mạng xây dựng kế hoạch hoạt động, tổ chức tập huấn, diễn tập, tổng hợp khó khăn, vướng mắc và đề xuất giải pháp nâng cao hiệu quả hoạt động của Đội.

4. Bộ phận hoặc đầu mối ứng cứu sự cố tại chỗ

- Người đứng đầu cơ quan, đơn vị, địa phương chỉ định bộ phận hoặc cá nhân làm đầu mối ứng cứu sự cố tại chỗ; căn cứ quy mô, tính chất và số lượng hệ thống thông tin, có thể thành lập tổ ứng cứu sự cố nội bộ theo thẩm quyền.

- Bộ phận hoặc đầu mối ứng cứu sự cố tại chỗ có trách nhiệm tiếp nhận cảnh báo, thực hiện biện pháp xử lý ban đầu, báo cáo, cung cấp nhật ký hệ thống và tài liệu có liên quan, duy trì hoạt động nghiệp vụ, phối hợp khôi phục hệ thống và chấp hành yêu cầu điều phối của Cơ quan thường trực, Đội ứng cứu sự cố.

- Danh sách đầu mối, phương tiện liên lạc, quyền truy cập khẩn cấp, vị trí thiết bị, bản sao lưu, sơ đồ hệ thống và quy trình vận hành thay thế được quản lý trong hồ sơ nội bộ, cập nhật ngay khi có thay đổi và cung cấp cho Công an tỉnh theo yêu cầu.

5. Các nhóm chức năng khi triển khai Phương án

a) Nhóm Chỉ đạo - điều phối - tổng hợp báo cáo

- Đơn vị chủ trì: Cơ quan thường trực của Đội ứng cứu sự cố; trường hợp cần huy động Đội, thực hiện theo quyết định của Đội trưởng Đội ứng cứu sự cố an ninh mạng; đối với trường hợp áp dụng mức huy động lực lượng Mức 3, phối hợp Văn phòng UBND tỉnh tham mưu công tác chỉ đạo, điều hành của UBND tỉnh.

- Đơn vị phối hợp: Cơ quan chủ quản, Đội ứng cứu sự cố, các sở, ngành liên quan.

- Nội dung thực hiện: Duy trì thông tin tổng hợp, đầy đủ và cập nhật về diễn biến sự cố; giao nhiệm vụ; thực hiện chế độ báo cáo; tham mưu quyết định và quản lý các thông tin nhận biết, nhận diện vụ việc, sự cố an toàn, an ninh mạng.

- Kết quả cần đạt: Nội dung chỉ đạo việc ứng cứu và khắc phục sự cố; nhật ký Chỉ đạo; báo cáo tình hình.

b) Nhóm kỹ thuật cô lập - khắc phục - khôi phục

- Đơn vị chủ trì: Đơn vị vận hành/chủ quản; Sở Khoa học và Công nghệ chủ trì phần hạ tầng dùng chung thuộc phạm vi quản lý.

- Đơn vị phối hợp: Đội ứng cứu sự cố; doanh nghiệp viễn thông, điện toán đám mây, phần mềm, thiết bị.

- Nội dung thực hiện: Cô lập; phân vùng; chặn địa chỉ, chỉ báo và dấu hiệu tấn công; vá, khắc phục lỗ hổng; gỡ bỏ mã độc; thay đổi khóa, mật khẩu; chuyển dự phòng; khôi phục và kiểm thử.

- Kết quả cần đạt: Kế hoạch kỹ thuật; biên bản thay đổi; kết quả kiểm thử.

c) Nhóm xác minh, điều tra, quản lý dữ liệu điện tử và xử lý vi phạm

- Đơn vị chủ trì: Công an tỉnh.

- Đơn vị phối hợp: Đội ứng cứu sự cố, cơ quan chủ quản, đơn vị vận hành, đơn vị cung cấp dịch vụ và các lực lượng chức năng khác có liên quan theo thẩm quyền.

- Nội dung thực hiện: Bảo vệ hiện trường; thu thập, bảo quản, bàn giao dữ liệu điện tử, tài liệu, thiết bị; phân tích, truy vết, xác minh hành vi và xử lý theo thẩm quyền.

- Kết quả cần đạt: Biên bản thu thập, bàn giao; dòng thời gian sự cố; kết quả xác minh.

d) Nhóm duy trì nghiệp vụ - dữ liệu - dịch vụ công

- Đơn vị chủ trì: Cơ quan chủ quản hệ thống/đơn vị quản lý trực tiếp.

- Đơn vị phối hợp: Văn phòng UBND tỉnh, Trung tâm Phục vụ hành chính công tỉnh, Sở Khoa học và Công nghệ, UBND các xã, phường.

- Nội dung thực hiện: Thực hiện quy trình thủ công hoặc các biện pháp

thay thế; xác định dữ liệu ưu tiên; đối soát hồ sơ, giao dịch, thời hạn; hỗ trợ người sử dụng.

- Kết quả cần đạt: Kế hoạch duy trì dịch vụ công; danh sách hồ sơ/giao dịch cần đối soát.

đ) Nhóm thông tin, truyền thông - hỗ trợ người dùng

- Đơn vị chủ trì: Cơ quan chủ quản; đối với trường hợp áp dụng mức huy động lực lượng Mức 3, thực hiện theo chỉ đạo của UBND tỉnh, Chủ tịch UBND tỉnh hoặc Phó Chủ tịch UBND tỉnh được phân công.

- Đơn vị phối hợp: Văn phòng UBND tỉnh, Sở Văn hóa, Thể thao và Du lịch, Công an tỉnh và cơ quan liên quan.

- Nội dung thực hiện: Thống nhất thông điệp; cảnh báo; hướng dẫn kênh thay thế; tiếp nhận phản ánh; ngăn tin giả và lừa đảo lợi dụng sự cố.

- Kết quả cần đạt: Thông báo được phê duyệt; nội dung hỏi - đáp; báo cáo phản ánh.

e) Nhóm hậu cần - tài chính - pháp lý - nhân lực

- Đơn vị chủ trì: Cơ quan chủ quản; Công an tỉnh đối với hoạt động của Đội ứng cứu sự cố.

- Đơn vị phối hợp: Sở Tài chính, Sở Nội vụ, Sở Tư pháp, đơn vị hậu cần và nhà cung cấp.

- Nội dung thực hiện: Bố trí địa điểm, thiết bị, phương tiện, ca trực, hợp đồng, thủ tục mua sắm hoặc thuê dịch vụ trong tình huống cấp bách, xử lý vấn đề pháp lý về dữ liệu và nhân lực.

- Kết quả cần đạt: Nguồn lực được huy động; hồ sơ chi phí, hợp đồng và quyết định nhân sự.

6. Cơ chế phối hợp và huy động

- Yêu cầu huy động thành viên Đội ứng cứu sự cố do Đội trưởng đội ứng cứu sự cố an ninh mạng hoặc người được ủy quyền quyết định trên cơ sở tham mưu của Công an tỉnh. Các yêu cầu cung cấp nhật ký hệ thống, thay đổi cấu hình, chặn kết nối, chuyển sang hệ thống dự phòng hoặc công bố thông tin được chuyển qua Cơ quan thường trực, Bộ phận Chỉ đạo, điều phối ứng cứu hoặc đầu mối được người có thẩm quyền xác định; trường hợp khẩn cấp có thể chỉ đạo bằng điện thoại hoặc kênh bảo mật nhưng phải được ghi nhận, xác nhận bằng văn bản hoặc nhật ký triển khai ứng cứu sau đó.

- Cơ quan, đơn vị được huy động cử người có thẩm quyền và năng lực; bảo đảm quyền truy cập cần thiết, thiết bị, tài liệu và khả năng làm việc liên tục; nếu không đáp ứng phải báo ngay lý do và đề xuất phương án thay thế.

- Doanh nghiệp viễn thông, điện toán đám mây, phần mềm, thiết bị và an ninh mạng thực hiện theo hợp đồng và yêu cầu hợp pháp; cung cấp nhật ký hệ thống, thông tin phiên bản, tài khoản hỗ trợ, bản vá, bản sạch, cấu hình, quan hệ phụ thuộc và báo cáo nguyên nhân.

- Sự cố liên quan hệ thống của bộ, ngành hoặc hạ tầng ngoài tỉnh được phối hợp qua cơ quan chủ quản, Công an tỉnh và đầu mối của bộ, ngành; không để việc chưa xác định trách nhiệm hợp đồng làm chậm biện pháp ngăn chặn cần thiết.

- Khi nhiều hệ thống thông tin bị ảnh hưởng, Công an tỉnh tổng hợp, tham mưu Đội trưởng đội ứng cứu sự cố an ninh mạng xác định thứ tự ưu tiên huy động, tổ chức lực lượng của Đội; trường hợp vượt thẩm quyền hoặc cần huy động nguồn lực liên ngành ở quy mô lớn thì báo cáo UBND tỉnh xem xét, chỉ đạo. Mỗi cơ quan chủ quản chỉ định một đầu mối thống nhất để cập nhật tình hình, tránh báo cáo trùng lặp qua nhiều kênh.

7. Bộ phận Chỉ đạo, điều phối ứng cứu, thông tin liên lạc và quản lý tình hình

- Đối với sự cố thuộc Mức 2, Mức 3, Công an tỉnh tham mưu Đội trưởng đội ứng cứu sự cố an ninh mạng hoặc UBND tỉnh thiết lập Bộ phận Chỉ đạo, điều phối ứng cứu, phòng điều phối trực tuyến hoặc tại hiện trường; xác định rõ người Chỉ đạo, thư ký, kênh liên lạc, thành phần tham gia, thời điểm cập nhật và yêu cầu bảo mật.

- Duy trì bảng tổng hợp tình hình, trong đó xác định thông tin nhận biết, nhận diện vụ việc/sự cố an ninh mạng, mức độ huy động lực lượng, hệ thống thông tin và dữ liệu bị ảnh hưởng, mục tiêu ưu tiên, nhiệm vụ đang thực hiện, quyết định đã ban hành, khó khăn, nhu cầu hỗ trợ và thời điểm dự kiến khôi phục.

- Kênh liên lạc chính do Công an tỉnh thông báo; bố trí kênh dự phòng khi thư điện tử, Internet hoặc hệ thống liên lạc bị xâm nhập. Thông tin thuộc bí mật nhà nước, dữ liệu cá nhân nhạy cảm, dữ liệu điện tử và tài liệu phục vụ xác minh, điều tra không được gửi qua nhóm trao đổi, thư điện tử hoặc nền tảng không đáp ứng yêu cầu bảo mật.

- Tần suất cập nhật mặc định: khi thực hiện ứng cứu sự cố: tần suất cập nhật ở mức 1 tùy theo yêu cầu của cơ quan chủ quản; sự cố mức 2 yêu cầu ít nhất 60 phút một lần trong 04 giờ đầu; sự cố mức 3 ít nhất 30 phút một lần hoặc theo chỉ đạo. Khi có thay đổi đột xuất phải báo cáo ngay, không chờ đến kỳ cập nhật.

- Thư ký Bộ phận Chỉ đạo, điều phối ứng cứu ghi đầy đủ nhật ký chỉ đạo, nhiệm vụ được giao, người tiếp nhận, thời hạn, kết quả và vấn đề còn tồn đọng; khi kết thúc ca trực phải thực hiện bàn giao bằng biên bản hoặc nhật ký điện tử.

8. Phát ngôn, cung cấp thông tin và hỗ trợ người dân, doanh nghiệp

- Cơ quan chủ quản dự thảo nội dung liên quan dịch vụ và người dùng; Công an tỉnh đánh giá yêu cầu bảo mật, điều tra, bảo vệ dữ liệu; cơ quan có thẩm quyền phê duyệt trước khi công bố.

- Đối với trường hợp áp dụng mức huy động lực lượng Mức 3 hoặc sự cố có tác động xã hội lớn, việc cung cấp thông tin thực hiện theo chỉ đạo của UBND tỉnh; Sở Văn hóa, Thể thao và Du lịch phối hợp hướng dẫn báo chí, thông tin điện tử, thông tin cơ sở theo chức năng.

- Nội dung công khai tập trung vào phạm vi dịch vụ bị ảnh hưởng, biện pháp bảo vệ người sử dụng, kênh thay thế và thời điểm cập nhật tiếp theo; không công bố sơ đồ hệ thống, lỗ hổng bảo mật, chỉ báo hoặc dấu hiệu xâm nhập có tính nhạy cảm, dữ liệu cá nhân hoặc thông tin có thể cản trở việc xác minh, điều tra.

- Tổ chức đầu mối tiếp nhận phản ánh, hỗ trợ hồ sơ, giao dịch và cảnh báo lừa đảo lợi dụng sự cố; thống kê phản ánh để phục vụ đánh giá tác động và khắc phục.

IV. XÁC ĐỊNH MỨC ĐỘ HUY ĐỘNG LỰC LƯỢNG, ĐIỀU KIỆN VÀ TRÌNH TỰ TRIỂN KHAI ỨNG CỨU

1. Tiêu chí xác định mức độ huy động lực lượng phục vụ ứng cứu sự cố

Mức độ huy động lực lượng được xác định trên cơ sở tổng hợp các tiêu chí về phạm vi ảnh hưởng, mức độ gián đoạn dịch vụ, nguy cơ đối với dữ liệu, tính chất sự cố, khả năng xử lý và yêu cầu Chỉ đạo. Khi các tiêu chí thuộc nhiều cấp khác nhau thì áp dụng cấp cao hơn cho đến khi có đủ căn cứ điều chỉnh xuống mức huy động lực lượng thấp hơn.

a) Mức 1 - Huy động lực lượng xử lý tại chỗ

- Phạm vi: Một thiết bị, tài khoản hoặc chức năng; không lan rộng.

- Dịch vụ: Không gián đoạn hoặc gián đoạn ngắn, có phương án thay thế.

- Dữ liệu: Không có dấu hiệu truy cập dữ liệu nhạy cảm; tính toàn vẹn được bảo đảm.

- Tính chất: Lỗi kỹ thuật, lỗi người dùng hoặc tấn công đã chặn, không duy trì.

- Khả năng xử lý: Đơn vị nội bộ xử lý được theo quy trình chuẩn.

- Chỉ đạo: Người đứng đầu/Chỉ đạo hệ thống tại chỗ.

b) Mức 2 - Huy động phối hợp cấp tỉnh

- Phạm vi: Một hệ thống hoặc nhiều đơn vị liên quan; phạm vi chưa xác định đầy đủ.

- Dịch vụ: Gián đoạn đáng kể, vượt ngưỡng nội bộ hoặc ảnh hưởng nhiều người dùng.

- Dữ liệu: Có nguy cơ lộ, mất, sửa dữ liệu; chưa xác định phạm vi hoặc liên

quan dữ liệu cá nhân nhạy cảm.

- Tính chất: Có dấu hiệu xâm nhập, mã độc, chiếm quyền, di chuyển ngang, tấn công có tổ chức.

- Khả năng xử lý: Cần Công an tỉnh, Đội ứng cứu sự cố, nhà cung cấp hoặc phối hợp liên ngành.

- Chỉ đạo: Cơ quan chủ quản chịu trách nhiệm chỉ đạo tại chỗ và quyết định các vấn đề về duy trì, tạm dừng, chuyển dự phòng, khôi phục hệ thống thuộc phạm vi quản lý; Công an tỉnh, với tư cách Cơ quan thường trực, tham mưu Đội trưởng Đội ứng cứu sự cố an ninh mạng huy động lực lượng và điều phối chuyên môn về an ninh mạng theo chức năng, thẩm quyền.

c) Mức 3 - Huy động khẩn cấp, diện rộng

- Phạm vi: Nhiều hệ thống, nhiều cơ quan, diện rộng hoặc có nguy cơ lan liên tỉnh/quốc gia.

- Dịch vụ: Tê liệt chỉ đạo điều hành, dịch vụ công, dịch vụ thiết yếu hoặc ảnh hưởng an toàn xã hội.

- Dữ liệu: Lộ bí mật nhà nước, dữ liệu quan trọng, dữ liệu cốt lõi hoặc dữ liệu cá nhân trên phạm vi lớn; dữ liệu trọng yếu bị sửa đổi, xóa hoặc phá hoại.

- Tính chất: Tấn công có chủ đích, phá hoại, gián điệp, mã độc tống tiền trên diện rộng hoặc xâm phạm hệ thống thông tin quan trọng.

- Khả năng xử lý: Vượt khả năng tỉnh hoặc cần Chỉ đạo cấp tỉnh, hỗ trợ cơ quan Trung ương.

- Chỉ đạo: Chủ tịch UBND tỉnh hoặc Phó Chủ tịch UBND tỉnh được phân công chỉ đạo chung đối với các nội dung cần điều phối, huy động nguồn lực cấp tỉnh; cơ quan chủ quản tiếp tục chịu trách nhiệm chỉ đạo tại chỗ đối với hệ thống thuộc phạm vi quản lý; Công an tỉnh tham mưu, điều phối chuyên môn về an ninh mạng; Đội trưởng Đội ứng cứu sự cố an ninh mạng tổ chức lực lượng của Đội theo quyết định huy động và chỉ đạo của cấp có thẩm quyền.

2. Trường hợp phải báo cáo ngay và xem xét nâng mức huy động lực lượng cao hơn

- Có dấu hiệu lộ, mất bí mật nhà nước; dữ liệu quan trọng, dữ liệu cốt lõi; dữ liệu cá nhân nhạy cảm hoặc dữ liệu cá nhân trên phạm vi lớn.

- Xuất hiện mã độc tống tiền, mã độc phá hoại; tài khoản quản trị, hạ tầng định danh, hệ thống sao lưu, mạng quản trị, nền tảng tích hợp và chia sẻ dữ liệu, cổng giao tiếp lập trình ứng dụng, hệ thống giám sát an ninh mạng, Trung tâm Điều hành thông minh hoặc Trung tâm dữ liệu bị xâm nhập, chiếm quyền hoặc gián đoạn nghiêm trọng.

- Gián đoạn dịch vụ công, hoạt động chỉ đạo điều hành, y tế cấp cứu, điện, nước, giao thông, thông tin liên lạc hoặc hệ thống phục vụ sự kiện chính trị quan trọng.

- Sau 60 phút kể từ khi xác minh mà chưa xác định được phạm vi ảnh hưởng; phát hiện dấu hiệu tấn công có hành vi lan truyền ngang trong hệ thống, truy cập thông qua tài khoản đơn vị cung cấp dịch vụ, tấn công chuỗi cung ứng, nguồn tấn công duy trì hoặc nhiều cơ quan cùng phát hiện một chỉ báo, dấu hiệu xâm nhập.

- Cơ quan, đơn vị không đủ nhân lực, công cụ, quyền truy cập hoặc bản sao lưu; nhà cung cấp không đáp ứng yêu cầu hỗ trợ; sự cố có nguy cơ kéo dài quá mục tiêu thời gian khôi phục hoặc vượt thẩm quyền, khả năng xử lý.

3. Thẩm quyền quyết định triển khai, điều chỉnh mức huy động lực lượng và kết thúc hoạt động ứng cứu sự cố

- Mức 1: Người đứng đầu cơ quan chủ quản hoặc người được ủy quyền quyết định huy động lực lượng tại chỗ, triển khai phương án nội bộ và chịu trách nhiệm báo cáo theo quy định.

- Mức 2: Cơ quan chủ quản quyết định các biện pháp vận hành đối với hệ thống thuộc phạm vi quản lý; Công an tỉnh xác minh, đánh giá yếu tố an ninh mạng, tham mưu Đội trưởng Đội ứng cứu sự cố an ninh mạng quyết định huy động thành viên Đội và tổ chức điều phối chuyên môn theo chức năng, thẩm quyền.

- Mức 3: Công an tỉnh tham mưu Chủ tịch UBND tỉnh hoặc Phó Chủ tịch UBND tỉnh được phân công chỉ đạo các nội dung cần điều phối, huy động nguồn lực cấp tỉnh; Đội trưởng Đội ứng cứu sự cố an ninh mạng tổ chức lực lượng của Đội; cơ quan chủ quản tiếp tục chỉ đạo tại chỗ và quyết định các vấn đề vận hành hệ thống thuộc phạm vi quản lý; việc đề nghị hỗ trợ Trung ương thực hiện theo thẩm quyền.

- Trong tình huống khẩn cấp chưa liên hệ được người có thẩm quyền, người đứng đầu đơn vị vận hành được thực hiện biện pháp cần thiết để ngăn thiệt hại rõ ràng, bảo đảm an toàn con người và bảo toàn dữ liệu điện tử, tài liệu, thiết bị phục vụ xác minh, điều tra; phải báo cáo ngay và chịu trách nhiệm về quyết định.

- Hạ mức hoặc kết thúc chỉ thực hiện khi phạm vi đã được kiểm soát, nguyên nhân trực tiếp đã được loại bỏ, dịch vụ và dữ liệu được xác minh, nguy cơ tái diễn ở mức chấp nhận và người có thẩm quyền đồng ý.

4. Nội dung và điều kiện triển khai hoạt động ứng cứu sự cố

- Thông tin nhận biết, nhận diện vụ việc/sự cố an ninh mạng, thời điểm triển khai, mức độ huy động lực lượng, hệ thống thông tin và phạm vi ảnh hưởng sơ bộ.

- Người chỉ đạo chung, người chỉ đạo tại chỗ, người chỉ đạo kỹ thuật, đầu mối Công an tỉnh và thành phần các nhóm chức năng.

- Mục tiêu trong 60 phút đầu và 04 giờ đầu; hệ thống thông tin, dịch vụ ưu tiên; hành động không được thực hiện hoặc phải được người có thẩm quyền phê duyệt trước khi thực hiện.

- Kênh điều phối, chế độ báo cáo, nơi tập kết, quyền truy cập và yêu cầu bảo mật.

- Nguồn lực được huy động, nhà cung cấp phải tham gia, thời điểm đánh giá lại và điều kiện đề nghị nâng lên mức huy động lực lượng cao hơn.

5. Trình tự triển khai ứng cứu sự cố

Hoạt động ứng cứu sự cố được thực hiện theo 08 giai đoạn dưới đây. Các mốc thời gian là mục tiêu phấn đấu để tổ chức lực lượng và kiểm soát tiến độ; người chỉ đạo được điều chỉnh theo diễn biến thực tế nhưng phải bảo đảm hoàn thành đầy đủ kết quả của từng giai đoạn:

a) Giai đoạn 1 - Phát hiện, ghi nhận và báo cáo ban đầu

- Mốc thời gian mục tiêu: 0 - 30 phút.

- Đơn vị chủ trì: Đơn vị vận hành/chủ quản.

- Đơn vị phối hợp: Công an tỉnh; bộ phận hoặc đầu mối ứng cứu sự cố tại chỗ.

- Kết quả cần đạt: Thông tin nhận biết, nhận diện vụ việc/sự cố an ninh mạng; hiện tượng; tài sản, tài khoản, dữ liệu; hành động ban đầu.

b) Giai đoạn 2 - Xác minh, phân loại và quyết định triển khai ứng cứu

- Mốc thời gian mục tiêu: 30 - 60 phút.

- Đơn vị chủ trì: Công an tỉnh phối hợp cơ quan chủ quản, tham mưu Đội trưởng đội ứng cứu sự cố an ninh mạng khi cần huy động nhân sự, thành viên của Đội ứng cứu sự cố.

- Đơn vị phối hợp: Đội ứng cứu sự cố, Sở Khoa học và Công nghệ, nhà cung cấp.

- Kết quả cần đạt: Mức huy động lực lượng; người Chỉ đạo; mục tiêu ưu tiên; lực lượng tham gia; kênh điều phối.

c) Giai đoạn 3 - Thực hiện ứng cứu ban đầu và bảo toàn hiện trạng

- Mốc thời gian mục tiêu: Trong 60 phút đầu.

- Đơn vị chủ trì: Đơn vị vận hành/Chỉ đạo kỹ thuật.

- Đơn vị phối hợp: Công an tỉnh, Đội ứng cứu sự cố.

- Kết quả cần đạt: Cô lập có kiểm soát; khóa tài khoản; nhật ký hệ thống, bộ nhớ, ảnh đĩa; duy trì dịch vụ tối thiểu.

d) Giai đoạn 4 – Thu thập, phân tích dữ liệu và phối hợp xác minh, điều tra

- Mốc thời gian mục tiêu: 01 - 04 giờ và liên tục.

- Đơn vị chủ trì: Công an tỉnh chủ trì hoặc phối hợp xác minh dấu hiệu, nguyên nhân, phạm vi ảnh hưởng của sự cố an ninh mạng; hướng dẫn bảo vệ hiện trường, bảo toàn dữ liệu điện tử, tài liệu, thiết bị có liên quan. Trường hợp phát hiện dấu hiệu vi phạm pháp luật, việc xác minh, điều tra, xử lý thực hiện theo chức năng, thẩm quyền và quy định của pháp luật; đơn vị vận hành có trách nhiệm cung cấp dữ liệu kỹ thuật theo yêu cầu hợp pháp của cơ quan có thẩm quyền.

- Đơn vị phối hợp: Đội ứng cứu sự cố, Sở Khoa học và Công nghệ, đơn vị cung cấp dịch vụ, chuyên gia trong lĩnh vực và các tổ chức, cá nhân liên quan.

- Kết quả cần đạt: Phạm vi ảnh hưởng; đường xâm nhập; chỉ báo, dấu hiệu xâm nhập; tài khoản, dữ liệu liên quan; dòng thời gian và nguyên nhân sơ bộ.

đ) Giai đoạn 5 - Ngăn chặn, loại bỏ nguyên nhân và khắc phục sự cố

- Mốc thời gian mục tiêu: 04 - 24 giờ hoặc theo thực tế.

- Đơn vị chủ trì: Đơn vị vận hành/chủ quản; Công an tỉnh điều phối.

- Đơn vị phối hợp: Đội ứng cứu sự cố, doanh nghiệp cung cấp dịch vụ.

- Kết quả cần đạt: Chặn địa chỉ và chỉ báo xâm nhập; gỡ bỏ mã độc; khắc phục lỗ hổng; thay đổi khóa, mật khẩu; thu hồi quyền; xây dựng lại thành phần bị xâm nhập.

e) Giai đoạn 6 – Duy trì hoạt động nghiệp vụ và khôi phục hệ thống, dịch vụ

- Mốc thời gian mục tiêu: Theo mục tiêu thời gian khôi phục, mục tiêu điểm khôi phục dữ liệu và thứ tự ưu tiên.

- Đơn vị chủ trì: Cơ quan chủ quản/đơn vị vận hành.

- Đơn vị phối hợp: Văn phòng UBND tỉnh, sở/ngành chuyên môn, Sở Khoa học và Công nghệ.

- Kết quả cần đạt: Kênh thay thế; bản sao sạch; đối soát dữ liệu, giao dịch, hồ sơ; dịch vụ ưu tiên hoạt động.

g) Giai đoạn 7 – Kiểm tra, đánh giá và quyết định kết nối hệ thống trở lại

- Mốc thời gian mục tiêu: Trước khi mở dịch vụ.

- Đơn vị chủ trì: Cơ quan chủ quản.

- Đơn vị phối hợp: Công an tỉnh, Đội ứng cứu sự cố đối với trường hợp áp dụng mức huy động lực lượng Mức 2 hoặc Mức 3 và đơn vị kiểm thử.

- Kết quả cần đạt: Kết quả kiểm tra độc lập; xác nhận nguyên nhân đã loại bỏ; kế hoạch mở kết nối từng phần.

h) Giai đoạn 8 – Tăng cường giám sát, kết thúc ứng cứu và rút kinh nghiệm

- Mốc thời gian mục tiêu: Tối thiểu 72 giờ hoặc theo rủi ro.

- Đơn vị chủ trì: Cơ quan chủ quản; Công an tỉnh, với tư cách Cơ quan thường trực, tổng hợp.

- Đơn vị phối hợp: Các đơn vị, tổ chức, cá nhân có liên quan.

- Kết quả cần đạt: Báo cáo kết thúc; nguyên nhân gốc rễ; xác định mức độ thiệt hại; kế hoạch khắc phục; bài học kinh nghiệm.

6. Yêu cầu chi tiết đối với xử lý ban đầu và bảo toàn dữ liệu điện tử, tài liệu, thiết bị phục vụ xác minh, điều tra

- Ghi nhận thời điểm phát hiện, nguồn cảnh báo, màn hình, tiến trình, kết nối, tài khoản, địa chỉ giao thức Internet, thay đổi gần nhất và người đang thao tác; kiểm tra, đồng bộ thời gian trước khi đối chiếu nhật ký hệ thống.

- Ưu tiên cô lập bằng biện pháp phân vùng mạng; áp dụng biện pháp chặn tại tường lửa, tường lửa ứng dụng web hoặc giải pháp phát hiện và ứng phó trên thiết bị đầu cuối; khóa tài khoản, thu hồi phiên đăng nhập hoặc ngắt kênh truy cập từ xa. Chỉ tắt nguồn thiết bị khi có nguy cơ mất an toàn vật lý, hoạt động phá hủy tiếp diễn không thể ngăn chặn bằng biện pháp khác hoặc theo yêu cầu của người có thẩm quyền.

- Thu thập trước các dữ liệu có khả năng mất nhanh, gồm dữ liệu trong bộ nhớ, tiến trình, kết nối, phiên đăng nhập và nhật ký hệ thống đang quay vòng; sau đó lập ảnh ổ đĩa hoặc bản sao, tính giá trị băm, niêm phong hoặc kiểm soát quyền truy cập và lập biên bản bàn giao.

- Không phân tích trực tiếp trên chứng cứ gốc khi có thể sử dụng bản sao; không dùng thiết bị lưu trữ chưa kiểm tra; không gửi mẫu mã độc, dữ liệu nhạy cảm qua kênh công cộng.

- Mọi thao tác của các đơn vị cung cấp dịch vụ, đơn vị có trách nhiệm bảo trì, vận hành hoặc tổ chức, cá nhân liên quan phải có người của đơn vị vận hành giám sát, ghi hình hoặc ghi nhật ký hệ thống khi phù hợp; tài khoản hỗ trợ chỉ cấp trong thời gian cần thiết và phải thu hồi sau sử dụng.

7. Xử lý sự cố liên quan dữ liệu, dữ liệu cá nhân và bí mật nhà nước

- Ngay khi có dấu hiệu truy cập, sao chép, truyền, sửa đổi hoặc làm mất dữ liệu trái phép, cơ quan chủ quản xác định loại dữ liệu, chủ thể dữ liệu, phạm vi ảnh hưởng, hệ thống nguồn, hệ thống nhận, quốc gia hoặc vùng lãnh thổ nơi lưu trữ, bên xử lý dữ liệu và khả năng dữ liệu tiếp tục bị khai thác.

- Công an tỉnh hướng dẫn hoặc chủ trì thu thập dữ liệu, tài liệu phục vụ xác minh, điều tra; thực hiện biện pháp ngăn truyền dữ liệu, truy vết và đánh giá yêu cầu báo cáo, thông báo theo quy định của pháp luật. Cơ quan chủ quản chịu trách

nhiệm thực hiện nghĩa vụ đối với chủ thể dữ liệu, cơ quan quản lý nhà nước và các bên có liên quan.

- Đối với bí mật nhà nước, áp dụng ngay chế độ bảo vệ tương ứng; khoanh vùng người biết, thiết bị, tài liệu, kênh truyền; không đưa nội dung bí mật vào báo cáo thông thường hoặc cuộc họp trực tuyến không đủ điều kiện.

- Thông báo cho cá nhân, tổ chức bị ảnh hưởng chỉ thực hiện khi có căn cứ, nội dung và thẩm quyền phù hợp; phải cân bằng yêu cầu bảo vệ quyền lợi với yêu cầu điều tra, an ninh, trật tự và tránh làm tăng nguy cơ lừa đảo.

8. Khôi phục, kiểm thử và kết nối lại

- Chỉ khôi phục từ bản sao, ảnh chuẩn, mã nguồn hoặc gói cài đặt đã kiểm tra; không khôi phục nguyên trạng một hệ thống bị xâm nhập mà chưa loại bỏ đường xâm nhập, tài khoản, khóa và cơ chế duy trì.

- Khôi phục theo quan hệ phụ thuộc, ưu tiên hạ tầng định danh, phân giải tên miền, đồng bộ thời gian, mạng quản trị, nền tảng ảo hóa, lưu trữ, cơ sở dữ liệu, nền tảng tích hợp và ứng dụng nghiệp vụ; kiểm thử đầy đủ chức năng, an ninh mạng, hiệu năng, nhật ký hệ thống và khả năng sao lưu.

- Đối soát dữ liệu trước và sau sự cố, giao dịch trong thời gian gián đoạn, hồ sơ xử lý thủ công, chữ ký số, thời hạn và trạng thái; xác định phần dữ liệu phải khôi phục, nhập lại hoặc xác minh với người dùng.

- Mở kết nối theo từng phần, ưu tiên nhóm người sử dụng hoặc đơn vị thử nghiệm; tăng cường giám sát thiết bị đầu cuối, sự kiện an ninh, tường lửa ứng dụng web, hệ thống quản lý danh tính, lưu lượng mạng và tài khoản đặc quyền; chuẩn bị sẵn phương án cô lập lại khi phát hiện dấu hiệu bất thường.

- Đối với trường hợp áp dụng mức huy động lực lượng Mức 2 hoặc Mức 3, cơ quan chủ quản quyết định kết nối lại hệ thống sau khi tham khảo ý kiến của Công an tỉnh và Đội ứng cứu sự cố về rủi ro an ninh mạng; quyết định kết nối lại và rủi ro còn lại phải được ghi nhận trong hồ sơ sự cố.

9. Chế độ báo cáo và hồ sơ sự cố

a) Báo cáo ban đầu

- Thời gian thực hiện: Không quá 30 phút kể từ khi phát hiện sự cố đối với trường hợp áp dụng mức huy động lực lượng Mức 2 hoặc Mức 3.

- Nội dung chủ yếu: Hiện tượng, thời điểm, hệ thống, dữ liệu, phạm vi sơ bộ, biện pháp đã làm, đầu mối và nhu cầu hỗ trợ.

- Hình thức và căn cứ thực hiện: Theo Phụ lục 2 Kế hoạch số 150/KH-UBND và hướng dẫn của Công an tỉnh.

b) Báo cáo cập nhật

- Thời điểm thực hiện: Đối với trường hợp áp dụng mức huy động lực lượng Mức 2: tối thiểu 60 phút một lần trong 04 giờ đầu; đối với Mức 3: tối thiểu 30 phút một lần hoặc theo chỉ đạo.

- Nội dung chủ yếu: Diễn biến, quyết định, phạm vi, tác động, kết quả, trở ngại, kế hoạch kỳ tiếp theo và mốc khôi phục dự kiến.

- Hình thức và căn cứ thực hiện: Nhật ký Bộ phận Chỉ đạo, điều phối ứng cứu, biểu mẫu điện tử hoặc văn bản theo yêu cầu.

c) Báo cáo đề nghị hỗ trợ hoặc nâng lên mức huy động lực lượng cao hơn

- Thời điểm thực hiện: Ngay khi sự cố vượt khả năng xử lý, có nguy cơ không đáp ứng mục tiêu thời gian khôi phục hoặc xuất hiện tiêu chí phải nâng lên mức huy động lực lượng cao hơn.

- Nội dung chủ yếu: Năng lực còn thiếu, rủi ro nếu chậm, lực lượng/công cụ cần huy động, phạm vi quyền truy cập và đầu mối.

- Hình thức và căn cứ thực hiện: Công an tỉnh tổng hợp, tham mưu theo thẩm quyền.

d) Báo cáo kết thúc

- Thời điểm thực hiện: Sau khi đủ tiêu chí kết thúc; cập nhật lại khi có kết quả điều tra mới.

- Nội dung chủ yếu: Nguyên nhân, phạm vi ảnh hưởng, dữ liệu, thiệt hại, quá trình xử lý, thời gian, dữ liệu và tài liệu đã thu thập, biện pháp khắc phục và trách nhiệm có liên quan.

- Hình thức và căn cứ thực hiện: Theo Phụ lục 3 Kế hoạch số 150/KH-UBND và hồ sơ kèm theo.

10. Tiêu chí kết thúc và rút kinh nghiệm

- Nguồn tấn công, mã độc, tài khoản, lỗ hổng và cơ chế duy trì đã được loại bỏ hoặc kiểm soát bằng biện pháp tạm thời được phê duyệt.

- Phạm vi ảnh hưởng, dữ liệu bị tác động và thiệt hại đã được xác định ở mức đủ để quyết định; dịch vụ ưu tiên hoạt động ổn định, bản sao và kết quả đối soát được xác nhận.

- Không còn chỉ báo tái xâm nhập trong thời gian giám sát tăng cường; nhật ký hệ thống, chứng cứ và hồ sơ được bảo quản; nghĩa vụ báo cáo, thông báo và phối hợp điều tra đã được thực hiện.

- Có kế hoạch khắc phục nguyên nhân gốc, người chịu trách nhiệm, nguồn lực và thời hạn; tổ chức họp rút kinh nghiệm, cập nhật phương án, kịch bản, kiến trúc, hợp đồng và nội dung diễn tập.

V. PHƯƠNG ÁN ỨNG CỨU ĐỐI VỚI MỘT SỐ NHÓM TÌNH HUỐNG SỰ CỐ CỤ THỂ

Các nội dung dưới đây trình bày khái quát tình huống, cách thức xử lý và cơ chế phối hợp để áp dụng thống nhất trên địa bàn tỉnh; cơ quan chủ quản phải tiếp tục cụ thể hóa theo kiến trúc, dữ liệu, điều kiện vận hành và yêu cầu chuyên ngành của từng hệ thống thông tin.

1. Yêu cầu chung khi xây dựng và áp dụng phương án theo tình huống

- Đối với từng hệ thống thông tin, chương trình ứng dụng, cơ quan chủ quản phải xây dựng tình huống, kịch bản cụ thể và phương án ứng cứu tương ứng; xác định tiêu chí nhận biết, điều kiện triển khai Phương án, mức huy động lực lượng, đơn vị chủ trì, đơn vị phối hợp, thứ tự ưu tiên, biện pháp duy trì hoạt động và tiêu chí kết thúc.

- Khi xảy ra sự cố, căn cứ hiện tượng, phạm vi ảnh hưởng và quan hệ phụ thuộc để lựa chọn nhóm tình huống phù hợp; trường hợp có nhiều biểu hiện thì áp dụng đồng thời các biện pháp có liên quan, ưu tiên xử lý nguyên nhân có khả năng làm lây lan hoặc gây gián đoạn trên diện rộng.

- Quy trình chung gồm: phát hiện, báo cáo; xác minh, đánh giá; cô lập có kiểm soát và bảo toàn hiện trạng; thu thập, phân tích; ngăn chặn, loại bỏ nguyên nhân; duy trì nghiệp vụ, khôi phục, kiểm thử; giám sát tăng cường; tổng hợp, báo cáo và rút kinh nghiệm.

2. Tình huống sự cố do bị tấn công mạng

- Các tình huống chủ yếu gồm: tấn công từ chối dịch vụ; giả mạo; sử dụng mã độc; truy cập trái phép, chiếm quyền điều khiển; thay đổi trái phép giao diện; mã hóa phần mềm, dữ liệu, thiết bị; phá hoại thông tin, dữ liệu, phần mềm; nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu; tấn công kết hợp nhiều hình thức và các hình thức tấn công mạng khác.

- Ngay khi phát hiện, đơn vị vận hành thực hiện báo cáo, cô lập có kiểm soát vùng bị ảnh hưởng, khóa hoặc thu hồi phiên đăng nhập và tài khoản bị lợi dụng; bảo toàn nhật ký hệ thống, dữ liệu bộ nhớ, tệp tin nghi ngờ, thông tin kết nối và các dữ liệu liên quan; không tự ý tắt nguồn, cài đặt lại hoặc xóa dữ liệu khi chưa có ý kiến của người có thẩm quyền.

- Công an tỉnh tiếp nhận, xác minh, đánh giá, tham mưu huy động Đội ứng cứu sự cố; phối hợp với cơ quan chủ quản, đơn vị vận hành và doanh nghiệp cung cấp dịch vụ xác định đường xâm nhập, chỉ báo, dấu hiệu tấn công, phạm vi lây lan; áp dụng biện pháp ngăn chặn, bóc gỡ mã độc, khắc phục lỗ hổng, thay đổi mật khẩu, khóa bí mật, chứng thư số và thu hồi quyền truy cập không còn cần thiết.

- Việc khôi phục chỉ được thực hiện từ bản sao lưu, mã nguồn hoặc bộ cài đặt đã được kiểm tra an toàn; phải đối soát dữ liệu, kiểm thử chức năng, bảo mật, hiệu năng, nhật ký và sao lưu trước khi kết nối trở lại; tăng cường giám sát để kịp thời phát hiện dấu hiệu tái xâm nhập.

3. Tình huống sự cố do lỗi hệ thống, thiết bị, phần mềm hoặc hạ tầng kỹ thuật

- Các tình huống chủ yếu gồm: sự cố nguồn điện, hệ thống làm mát; mất hoặc suy giảm kết nối Internet, mạng truyền số liệu chuyên dùng, mạng riêng ảo, dịch vụ phân giải tên miền; lỗi phần mềm, phần cứng, ứng dụng, nền tảng ảo hóa, lưu trữ, sao lưu; quá tải hệ thống; sự cố dịch vụ điện toán đám mây, nhà cung cấp hoặc hạ tầng kỹ thuật khác.

- Đơn vị vận hành chủ trì kiểm tra phạm vi ảnh hưởng, xác định thành phần hư hỏng hoặc suy giảm, triển khai thiết bị, đường truyền, nguồn điện hoặc hệ thống dự phòng; phối hợp Sở Khoa học và Công nghệ, doanh nghiệp viễn thông, điện lực, điện toán đám mây, nhà cung cấp thiết bị và phần mềm để khắc phục theo phạm vi trách nhiệm.

- Trường hợp chưa xác định rõ nguyên nhân kỹ thuật hay có dấu hiệu bị tấn công, phải giữ nguyên nhật ký, cấu hình, lịch sử thay đổi và báo cáo Công an tỉnh; không mặc nhiên kết luận là lỗi kỹ thuật để bỏ qua việc xác minh nguy cơ xâm nhập, phá hoại hoặc tấn công chuỗi cung ứng.

- Trong thời gian khắc phục, cơ quan chủ quản tổ chức duy trì hoạt động bằng hệ thống dự phòng, đường truyền thay thế hoặc quy trình thủ công; sau khi khôi phục phải kiểm tra quan hệ phụ thuộc, đối soát dữ liệu, giao dịch và đánh giá khả năng đáp ứng mục tiêu thời gian khôi phục, mục tiêu điểm khôi phục dữ liệu.

4. Tình huống sự cố do lỗi của người quản trị, vận hành hoặc người sử dụng

- Các tình huống chủ yếu gồm: sai sót khi cập nhật, thay đổi, cấu hình phần cứng hoặc phần mềm; không tuân thủ chính sách, quy trình bảo đảm an ninh mạng; dừng dịch vụ không đúng thẩm quyền; chia sẻ, sử dụng chung tài khoản; làm lộ thông tin xác thực; thao tác nhầm, xóa hoặc sửa dữ liệu; lạm dụng tài khoản đặc quyền và các sai sót khác trong quản trị, vận hành, sử dụng hệ thống.

- Cơ quan chủ quản, đơn vị vận hành phải kịp thời dừng hoặc thu hồi quyền của tài khoản có liên quan, ghi nhận đầy đủ thao tác, lịch sử thay đổi và người thực hiện; khôi phục cấu hình, dữ liệu từ bản chuẩn đã được kiểm tra; đánh giá phạm vi ảnh hưởng và báo cáo Công an tỉnh khi có dấu hiệu cố ý, che giấu, chiếm đoạt, phá hoại hoặc làm lộ dữ liệu.

- Sau khi xử lý, khắc phục phải rà soát quy trình phê duyệt thay đổi, phân

quyền, giám sát tài khoản đặc quyền, cơ chế kiểm soát chéo, đào tạo người quản trị, vận hành, sử dụng nhằm khắc phục các điểm yếu về tổ chức, quản lý, ngăn ngừa tái diễn.

5. Tình huống sự cố liên quan đến dữ liệu và cơ sở dữ liệu

- Các tình huống chủ yếu gồm: dữ liệu cá nhân, dữ liệu quan trọng, dữ liệu cốt lõi hoặc bí mật nhà nước bị truy cập, sao chép, truyền đưa, công bố, sửa đổi hoặc làm mất trái phép; cơ sở dữ liệu đất đai, tài chính - ngân sách, hộ tịch, cán bộ, y tế, giáo dục và dữ liệu chuyên ngành bị xóa, sửa, làm sai lệch hoặc gian lận.

- Cơ quan chủ quản dữ liệu chủ trì xác định loại dữ liệu, chủ thể, phạm vi, hệ thống nguồn, hệ thống nhận, bên xử lý và khả năng dữ liệu tiếp tục bị khai thác; áp dụng biện pháp ngăn chặn truyền đưa, khóa tài khoản, bảo toàn nhật ký, bản sao, lịch sử giao dịch và tổ chức đối soát với nguồn dữ liệu có giá trị pháp lý.

- Công an tỉnh hướng dẫn hoặc chủ trì xác minh, thu thập dữ liệu, tài liệu phục vụ điều tra; hướng dẫn thực hiện nghĩa vụ báo cáo, thông báo theo pháp luật về dữ liệu, bảo vệ dữ liệu cá nhân và bảo vệ bí mật nhà nước. Việc thông báo cho tổ chức, cá nhân bị ảnh hưởng phải đúng thẩm quyền, nội dung và thời hạn; không làm cản trở hoạt động điều tra hoặc tạo điều kiện cho đối tượng xấu lợi dụng.

6. Tình huống thiên tai, hỏa hoạn, sự cố vật lý và hệ thống dịch vụ thiết yếu, công nghệ vận hành

- Các tình huống chủ yếu gồm: bão, lũ, sạt lở, ngập lụt, động đất, cháy, nổ, chập điện, hư hỏng hệ thống làm mát, mất khả năng tiếp cận phòng máy; sự cố đối với hệ thống điện, cấp nước, y tế cấp cứu, giao thông, công nghiệp, quan trắc, camera và hệ thống điều khiển giám sát, thu thập dữ liệu hoặc hệ thống điều khiển công nghiệp.

- Ưu tiên tuyệt đối an toàn tính mạng, sức khỏe con người, môi trường và an toàn công trình. Khi có cháy, nổ hoặc nguy cơ cứu nạn, cứu hộ, lực lượng Cảnh sát phòng cháy, chữa cháy và cứu nạn, cứu hộ chủ trì xử lý theo phương án chuyên ngành; lực lượng kỹ thuật chỉ tiếp cận, di chuyển hoặc khôi phục thiết bị sau khi hiện trường được xác định an toàn.

- Cơ quan, đơn vị chuyên ngành Chỉ đạo về an toàn vận hành và duy trì dịch vụ thiết yếu; Công an tỉnh điều phối về an ninh mạng; Sở Khoa học và Công nghệ, doanh nghiệp điện lực, viễn thông, cấp nước và đơn vị vận hành công trình phối hợp chuyển nguồn, chuyển địa điểm hoặc hệ thống dự phòng, vận hành thủ công và khôi phục theo thứ tự ưu tiên.

- Đối với hệ thống công nghệ vận hành, hệ thống điều khiển giám sát, hệ thống điều khiển công nghiệp và hệ thống có khả năng ảnh hưởng đến an toàn hóa chất, phòng cháy, chữa cháy, môi trường, điện, nước, giao thông hoặc hoạt động

sản xuất, việc ứng cứu sự cố phải tuân thủ quy trình an toàn chuyên ngành của đơn vị vận hành. Mọi biện pháp kỹ thuật có khả năng làm thay đổi trạng thái vận hành phải được phối hợp, phê duyệt và ghi nhận theo thẩm quyền, bảo đảm không gây nguy hiểm cho con người, công trình, môi trường và hoạt động sản xuất.

- Trước khi kết nối trở lại hệ thống công nghệ vận hành phải kiểm tra thiết bị điều khiển, cấu hình, tín hiệu, lệnh điều khiển, ranh giới giữa mạng công nghệ thông tin và mạng công nghệ vận hành; tổ chức kiểm thử chuyên ngành, giám sát tăng cường và sẵn sàng cô lập lại khi phát hiện bất thường.

7. Nguyên tắc lựa chọn kịch bản và điều chỉnh biện pháp thực hiện

- Kịch bản là nội dung hướng dẫn tổ chức thực hiện, không thay thế việc đánh giá tình hình thực tế. Người chỉ đạo được điều chỉnh thứ tự, thành phần lực lượng và biện pháp xử lý nhưng phải bảo đảm yêu cầu về an toàn con người, bảo toàn dữ liệu, tài liệu, thiết bị; duy trì dịch vụ, chế độ báo cáo và trách nhiệm của từng cơ quan, đơn vị.

- Mỗi cơ quan chủ quản phải cụ thể hóa kịch bản theo tên hệ thống, kiến trúc, tài khoản, mục tiêu thời gian khôi phục và mục tiêu điểm khôi phục dữ liệu, dữ liệu, thao tác kỹ thuật và đầu mối; phần hệ thống chứa thông tin nhạy cảm trong tài liệu nội bộ.

- Đối với sự cố xảy ra đồng thời, Công an tỉnh xác định vụ việc chính, các vụ việc có liên quan, chỉ báo hoặc dấu hiệu xâm nhập chung và cơ chế chia sẻ thông tin; ưu tiên xử lý điểm có khả năng gây lây lan hoặc thành phần có quan hệ phụ thuộc trước.

VI. TRÁCH NHIỆM CỦA CÁC CƠ QUAN, ĐƠN VỊ

1. UBND tỉnh, Chủ tịch UBND tỉnh

- Chỉ đạo chung công tác ứng cứu trên địa bàn; quyết định hoặc chỉ đạo việc huy động nguồn lực, ưu tiên dịch vụ, phối hợp liên ngành, thông tin công khai và đề nghị hỗ trợ Trung ương đối với trường hợp áp dụng mức huy động lực lượng Mức 3 theo thẩm quyền.

- Chỉ đạo người đứng đầu cơ quan, đơn vị thực hiện trách nhiệm, cung cấp nguồn lực và khắc phục tồn tại; xem xét trách nhiệm khi chậm báo cáo, không phối hợp, không tuân thủ chỉ đạo hoặc để tái diễn do không khắc phục.

- Chỉ đạo rà soát, cập nhật Phương án khi có thay đổi lớn về pháp luật, tổ chức bộ máy, hệ thống trọng điểm hoặc sau sự cố nghiêm trọng.

2. Đội ứng cứu sự cố an ninh mạng tỉnh Thanh Hóa

- Tổ chức thực hiện nhiệm vụ, quyền hạn theo Quyết định thành lập, Quy chế hoạt động của Đội và Phương án này; hỗ trợ các cơ quan, đơn vị, địa phương

trong phòng ngừa, phát hiện, ứng cứu, khắc phục sự cố an ninh mạng.

- Khi xảy ra sự cố cần huy động lực lượng cấp tỉnh, Đội trưởng đội ứng cứu sự cố an ninh mạng căn cứ đề xuất của Cơ quan thường trực để quyết định thành phần tham gia, phân công nhiệm vụ, tổ chức phối hợp với cơ quan chủ quản, đơn vị vận hành và các lực lượng có liên quan.

- Nghiên cứu, thu thập, xác minh, đánh giá, cảnh báo nguy cơ, sự cố, rủi ro an toàn, an ninh mạng; tham gia phân tích kỹ thuật, ngăn chặn, khắc phục, phục hồi hệ thống theo chức năng, nhiệm vụ và phân công của Đội trưởng đội ứng cứu sự cố an ninh mạng tỉnh.

- Phối hợp với lực lượng ứng cứu sự cố của các bộ, ngành, địa phương, cơ quan điều phối quốc gia và tổ chức, doanh nghiệp có năng lực khi được cơ quan có thẩm quyền yêu cầu; thực hiện nghiêm chế độ bảo mật và quản lý dữ liệu, tài liệu trong quá trình phối hợp.

- Hằng năm xây dựng, tổ chức thực hiện kế hoạch hoạt động; tham gia bồi dưỡng, tập huấn, đào tạo, hội thảo, diễn tập; tổng hợp khó khăn, vướng mắc, báo cáo và đề xuất giải pháp nâng cao hiệu quả công tác ứng cứu sự cố trên địa bàn tỉnh.

- Đội trưởng đội ứng cứu sự cố an ninh mạng chịu trách nhiệm trước Chủ tịch UBND tỉnh về toàn bộ hoạt động của Đội; thành viên Đội làm việc theo chế độ kiêm nhiệm, thực hiện nhiệm vụ theo phân công và chịu trách nhiệm về nội dung công việc được giao.

- Việc sử dụng bộ máy, phương tiện, con dấu và các điều kiện phục vụ hoạt động của Đội thực hiện theo Quyết định thành lập Đội, Quy chế hoạt động do Đội trưởng đội ứng cứu sự cố an ninh mạng ban hành và quy định của pháp luật có liên quan.

3. Công an tỉnh - Cơ quan thường trực của Đội ứng cứu sự cố an ninh mạng tỉnh, Cơ quan Thường trực Tiểu ban An ninh mạng tỉnh

- Thực hiện nhiệm vụ Cơ quan thường trực của Đội ứng cứu sự cố; giao Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao làm bộ phận giúp việc, thường trực; tham mưu Đội trưởng đội ứng cứu sự cố an ninh mạng ban hành Quy chế hoạt động, phân công nhiệm vụ và tổ chức triển khai hoạt động của Đội.

- Tiếp nhận, xác nhận, đánh giá thông tin về sự cố; xác minh, đánh giá yếu tố an ninh mạng; tham mưu Đội trưởng Đội ứng cứu sự cố an ninh mạng huy động thành viên Đội và tham mưu UBND tỉnh chỉ đạo đối với sự cố vượt khả năng xử lý của cơ quan chủ quản hoặc cần huy động, điều phối nguồn lực cấp tỉnh.

- Chủ trì điều phối chuyên môn về an ninh mạng; hướng dẫn bảo vệ hiện

trường, bảo toàn dữ liệu điện tử, tài liệu, thiết bị; chủ trì hoặc phối hợp xác minh, truy vết, ngăn chặn nguồn tấn công và xử lý hành vi vi phạm theo chức năng, thẩm quyền. Trường hợp có dấu hiệu tội phạm, thực hiện các hoạt động điều tra theo quy định của pháp luật về tố tụng hình sự.

- Theo dõi, tổng hợp diễn biến, kết quả ứng cứu; cảnh báo nguy cơ, phương thức, thủ đoạn và biện pháp phòng ngừa cho các cơ quan, đơn vị có liên quan; tổng hợp báo cáo UBND tỉnh, Bộ Công an và đề nghị hỗ trợ Trung ương khi cần thiết.

- Tham mưu Đội trưởng đội ứng cứu sự cố an ninh mạng xây dựng kế hoạch hoạt động hằng năm; tổ chức tập huấn, huấn luyện, diễn tập; quản lý danh sách thành viên, tiếp nhận thông báo thay đổi nhân sự; theo dõi việc thực hiện nhiệm vụ và kế hoạch khắc phục sau sự cố.

- Khi sự cố an ninh mạng đồng thời phát sinh cháy, nổ, khói, ngập nước, chập điện hoặc nguy cơ trực tiếp đối với tính mạng, sức khỏe con người, chỉ đạo lực lượng Cảnh sát phòng cháy, chữa cháy và cứu nạn, cứu hộ chủ trì thực hiện nhiệm vụ theo pháp luật và phương án chuyên ngành; lực lượng kỹ thuật chỉ tiếp cận, di chuyển hoặc khôi phục thiết bị khi hiện trường đã được xác định bảo đảm an toàn.

4. Sở Khoa học và Công nghệ

- Tổ chức quản lý, vận hành an toàn hạ tầng số, Trung tâm dữ liệu, mạng truyền số liệu chuyên dùng, nền tảng tích hợp, chia sẻ dữ liệu, hệ thống dùng chung và các hệ thống thuộc phạm vi được giao; duy trì sơ đồ quan hệ phụ thuộc, phương án sao lưu và đầu mối kỹ thuật có khả năng tiếp nhận, xử lý yêu cầu 24 giờ trong ngày, 07 ngày trong tuần.

- Khi xảy ra sự cố, chủ trì xử lý kỹ thuật đối với hạ tầng, nền tảng, hệ thống dùng chung thuộc phạm vi được giao quản lý; phối hợp Công an tỉnh thực hiện cô lập, trích xuất nhật ký hệ thống, đánh giá phạm vi liên hệ thống, chuyển dự phòng, khôi phục và giám sát sau phục hồi; trường hợp có dấu hiệu tấn công hoặc chưa loại trừ yếu tố an ninh mạng, kịp thời phối hợp Công an tỉnh xác minh, xử lý.

- Huy động đơn vị vận hành, doanh nghiệp viễn thông, điện toán đám mây, phần mềm, thiết bị; cung cấp cấu hình, nhật ký, hợp đồng và chuyên gia; không để các đơn vị cung cấp dịch vụ bảo trì, vận hành tự xử lý hoặc công bố thông tin ngoài cơ chế điều phối.

- Rà soát kiến trúc, tiêu chuẩn kỹ thuật, năng lực dự phòng, sao lưu và quan hệ phụ thuộc sau sự cố; đề xuất đầu tư, nâng cấp và khắc phục điểm yếu.

5. Văn phòng UBND tỉnh và Trung tâm Phục vụ hành chính công tỉnh

- Phối hợp bảo đảm hoạt động chỉ đạo, điều hành; hệ thống quản lý văn bản,

kênh thông tin phục vụ lãnh đạo, hệ thống giải quyết thủ tục hành chính và các kênh phục vụ người dân, doanh nghiệp thuộc phạm vi quản lý.

- Chủ trì hoặc phối hợp triển khai phương án duy trì nghiệp vụ, tiếp nhận hồ sơ và xử lý công việc thay thế; xác định hồ sơ, giao dịch, thời hạn cần bảo vệ và đối soát sau khôi phục.

- Phối hợp Công an tỉnh tổng hợp tình hình, tham mưu báo cáo lãnh đạo UBND tỉnh; đối với hệ thống, dịch vụ thuộc phạm vi quản lý, phối hợp cơ quan chủ quản thông báo tình trạng dịch vụ, kênh thay thế và hướng dẫn người dân, doanh nghiệp.

- Cử cán bộ nghiệp vụ tham gia kiểm thử, xác nhận chức năng, chữ ký số, trạng thái hồ sơ và kết quả giải quyết trước khi đưa hệ thống trở lại hoạt động.

6. Sở Văn hóa, Thể thao và Du lịch

Phối hợp hướng dẫn các cơ quan báo chí, trang thông tin điện tử, hệ thống thông tin cơ sở và các kênh thông tin đối ngoại thực hiện công tác thông tin, truyền thông khi xảy ra sự cố có tác động xã hội; tăng cường rà soát, phát hiện và phối hợp xử lý thông tin giả mạo, sai lệch, thông tin lừa đảo liên quan đến sự cố. Phối hợp với cơ quan chủ quản, Công an tỉnh và Văn phòng UBND tỉnh xây dựng, thống nhất thông điệp truyền thông, lựa chọn kênh thông tin phù hợp và chuẩn bị nội dung hỏi - đáp. Không cung cấp, công bố thông tin, dữ liệu, chi tiết kỹ thuật hoặc nội dung liên quan đến kết quả điều tra khi chưa được cơ quan có thẩm quyền phê duyệt.

7. Sở Nội vụ và Sở Tư pháp

- Sở Nội vụ: phối hợp bố trí, huy động nhân lực; hướng dẫn xử lý về cán bộ, công chức, viên chức, kỷ luật, điều động hoặc đình chỉ quyền truy cập khi có yêu cầu hợp pháp; bảo đảm quyền và lợi ích của người có liên quan.

- Sở Tư pháp: phối hợp rà soát, tham gia ý kiến về mặt pháp lý đối với các nội dung, văn bản liên quan đến công tác ứng cứu sự cố an ninh mạng theo chức năng, nhiệm vụ và thẩm quyền do pháp luật quy định.

8. Các sở, ngành có nhiệm vụ quản lý nhà nước trong các lĩnh vực chuyên ngành liên quan đến hoạt động ứng cứu sự cố

- Sở Y tế: chỉ đạo cơ sở y tế duy trì cấp cứu, khám chữa bệnh, xét nghiệm, dược, hồ sơ bệnh án và thiết bị y tế; xác định dữ liệu sức khỏe ưu tiên, phối hợp bảo vệ dữ liệu cá nhân nhạy cảm và kiểm thử an toàn trước khi khôi phục.

- Sở Tài chính: Hướng dẫn theo chức năng, nhiệm vụ, thẩm quyền việc quản lý, sử dụng và quyết toán kinh phí liên quan đến hoạt động ứng cứu sự cố trên địa bàn tỉnh.

- Sở Giáo dục và Đào tạo: Bảo đảm tính liên tục và an toàn cho các hệ thống thông tin phục vụ công tác thi, tuyển sinh; chỉ đạo các cơ sở giáo dục thuộc thẩm quyền quản lý trên địa bàn tỉnh tuân thủ quy định về dữ liệu kết quả học tập, dữ liệu cá nhân của giáo viên, học sinh; tổ chức đối soát kết quả xử lý sự cố và thông báo cho các đơn vị liên quan theo chức năng, nhiệm vụ, thẩm quyền được giao.

- Sở Nông nghiệp và Môi trường: duy trì hoạt động hệ thống thông tin về đất đai, tài nguyên, môi trường, quan trắc, thủy lợi và cơ sở dữ liệu chuyên ngành; phối hợp xác minh dữ liệu, bản đồ, hồ sơ và tín hiệu quan trắc.

- Sở Công Thương: theo chức năng, nhiệm vụ được giao, phối hợp với Công an tỉnh, Sở Khoa học và Công nghệ và các cơ quan, đơn vị liên quan hướng dẫn, đôn đốc các đơn vị hoạt động trong lĩnh vực điện lực, năng lượng, công nghiệp, cụm công nghiệp và thương mại xây dựng, cập nhật phương án ứng cứu sự cố; phối hợp duy trì hoạt động cung ứng điện, xăng dầu, hàng hóa thiết yếu và bảo đảm an toàn, cung cấp đầu mối, thông tin chuyên ngành và tham gia ứng cứu khi có yêu cầu của cơ quan có thẩm quyền.

- Sở Xây dựng, Ban Quản lý Khu kinh tế Nghi Sơn và các khu công nghiệp và cơ quan liên quan thực hiện phối hợp trong phạm vi chức năng, nhiệm vụ, quyền hạn được giao đối với giao thông, hạ tầng kỹ thuật, công trình, khu công nghiệp, hệ thống điều khiển, hệ thống điều khiển giám sát, hệ thống điều khiển công nghiệp và dịch vụ thiết yếu thuộc phạm vi quản lý.

- Các sở, ngành khác: chịu trách nhiệm về dữ liệu, hệ thống và đơn vị trực thuộc; cử chuyên gia nghiệp vụ, xác định dịch vụ ưu tiên, duy trì quy trình thay thế và đối soát sau khôi phục.

9. Cơ quan, đơn vị, địa phương có thành viên tham gia Đội ứng cứu sự cố

- Cử nhân sự có năng lực, phù hợp tham gia Đội ứng cứu sự cố; kịp thời cử người thay thế và thông báo cho Cơ quan thường trực khi có thay đổi về nhân sự, vị trí công tác hoặc khả năng tham gia.

- Khi nhận được thông báo của Cơ quan thường trực hoặc yêu cầu của Đội trưởng đội ứng cứu sự cố an ninh mạng, ưu tiên bố trí thành viên tham gia; bảo đảm thời gian, phương tiện, trang thiết bị, quyền tiếp cận và các điều kiện cần thiết để thực hiện nhiệm vụ.

- Quản lý, đánh giá việc thực hiện nhiệm vụ của thành viên thuộc cơ quan, đơn vị; phối hợp xử lý các vấn đề về chế độ, chính sách, bảo mật, bàn giao công việc và trách nhiệm phát sinh trong thời gian tham gia ứng cứu sự cố.

10. UBND các xã, phường

- Người đứng đầu chịu trách nhiệm đối với hệ thống, thiết bị, dữ liệu và tài

khoản tại địa phương; chỉ định lãnh đạo, cán bộ kỹ thuật và người thay thế; duy trì phương án liên lạc, tiếp nhận hồ sơ và phục vụ người dân khi hệ thống tập trung gián đoạn.

- Khi phát hiện thiết bị hoặc tài khoản bị ảnh hưởng, thực hiện biện pháp cô lập an toàn và báo cáo ngay; không tự ý cài đặt lại máy, xóa dữ liệu, thuê đơn vị bên ngoài hoặc công bố thông tin; bố trí hiện trường, thiết bị, nhật ký hệ thống và cán bộ để phối hợp xử lý.

- Thực hiện hướng dẫn của Công an tỉnh, Sở Khoa học và Công nghệ và cơ quan chủ quản hệ thống; thông báo kênh phục vụ thay thế; đối soát hồ sơ, dữ liệu và giao dịch sau khôi phục.

- Tổ chức tuyên truyền, tập huấn, diễn tập; cập nhật danh sách đầu mối khi thay đổi nhân sự và bố trí kinh phí trong dự toán hằng năm.

11. Cơ quan chủ quản hệ thống thông tin

- Chịu trách nhiệm cuối cùng về an ninh mạng, dữ liệu, tính liên tục của dịch vụ và nghĩa vụ đối với người dùng; ban hành phương án nội bộ, phân loại hệ thống thông tin, xác định mục tiêu thời gian khôi phục và mục tiêu điểm khôi phục dữ liệu, phương án sao lưu, khôi phục sau sự cố và hợp đồng ràng buộc trách nhiệm với đơn vị hỗ trợ bảo trì, vận hành.

- Khi xảy ra sự cố, quyết định mục tiêu nghiệp vụ, việc duy trì, tạm dừng hoặc chuyển sang hệ thống dự phòng; phân công người chỉ đạo tại chỗ, huy động nguồn lực, thực hiện báo cáo và phối hợp ứng cứu; không che giấu hoặc trì hoãn báo cáo vì chưa xác định được trách nhiệm.

- Phê duyệt khôi phục, kết nối lại, thông báo người dùng và kế hoạch khắc phục; tổ chức rút kinh nghiệm, xác định trách nhiệm và báo cáo kết quả theo yêu cầu.

12. Đơn vị vận hành hệ thống thông tin

- Giám sát, phát hiện, ghi nhận và xử lý an toàn ban đầu; duy trì nhật ký, sơ đồ, cấu hình, danh mục tài sản, tài khoản, bản sao và công cụ; báo cáo ngay cho đơn vị chủ quản và đầu mối Đội ứng cứu sự cố.

- Thực hiện cô lập, thu thập dữ liệu kỹ thuật, bảo toàn hiện trạng, chặn, vá, gỡ mã độc, khôi phục và kiểm thử theo chỉ đạo triển khai ứng cứu; quản lý chặt tài khoản khẩn cấp và thao tác của các bên liên quan.

- Cung cấp đầy đủ nhật ký hệ thống, thiết bị, ảnh hệ thống, tài khoản, lịch sử thay đổi và nhân sự; lập biên bản mọi thay đổi; duy trì giám sát sau khôi phục và báo cáo bất thường.

13. Doanh nghiệp viễn thông, điện, nước, điện toán đám mây, công nghệ, an ninh mạng

- Duy trì đầu mối có khả năng tiếp nhận, xử lý yêu cầu 24 giờ trong ngày, 07 ngày trong tuần và khả năng hỗ trợ theo thỏa thuận mức dịch vụ; thông báo ngay khi phát hiện sự cố liên quan đến sản phẩm, hạ tầng hoặc các yếu tố thuộc chuỗi cung ứng sản phẩm, hạ tầng, dịch vụ an ninh mạng có thể ảnh hưởng đến hệ thống thông tin của tỉnh.

- Theo yêu cầu có trách nhiệm cung cấp nhật ký hệ thống, dữ liệu kết nối, phiên bản, cấu hình, đặc điểm hệ thống, bản vá, tài khoản hỗ trợ, thông tin về các đơn vị cung cấp dịch vụ bảo trì, vận hành liên quan, bản sao hệ thống, các chỉ báo xâm nhập hệ thống thông tin và có trách nhiệm báo cáo trung thực nguyên nhân; phối hợp ngăn chặn tấn công mạng.

- Công ty Điện lực Thanh Hóa và đơn vị trực tiếp cung cấp điện có trách nhiệm phối hợp kiểm tra, cô lập sự cố điện, chuyển nguồn, ưu tiên khôi phục cấp điện và cung cấp thông tin vận hành đối với Trung tâm dữ liệu, trung tâm điều hành, hệ thống thông tin và dịch vụ thiết yếu khi được cơ quan có thẩm quyền yêu cầu.

- Không tự ý xóa dữ liệu, thay đổi hệ thống, công bố thông tin, liên hệ đối tượng tấn công hoặc đưa nhân sự không được phê duyệt vào xử lý; bảo đảm hồ sơ, biên bản thu thập và bàn giao dữ liệu, tài liệu, thiết bị và trách nhiệm đối với thao tác của nhân sự.

- Quy định rõ về nghĩa vụ và trách nhiệm trong bảo đảm an ninh mạng, bảo vệ dữ liệu, thời hạn thông báo, quyền kiểm tra, nghĩa vụ cung cấp nhật ký hệ thống và dữ liệu, tài liệu phục vụ xác minh, điều tra trong hợp đồng cung cấp dịch vụ; hỗ trợ khẩn cấp, chuyển giao dữ liệu, kế hoạch kết thúc hoặc chuyển đổi dịch vụ và trách nhiệm bồi thường.

14. Cán bộ, công chức, viên chức, người lao động và người sử dụng

- Tuân thủ quy chế sử dụng hệ thống, bảo vệ mật khẩu, mã xác thực, thiết bị ký số, dữ liệu; không cài phần mềm, sử dụng dịch vụ lưu trữ, chuyển dữ liệu hoặc chia sẻ tài khoản trái quy định.

- Báo ngay các vấn đề nghi ngờ như thư điện tử, liên kết, tệp, đăng nhập, cuộc gọi, giao dịch hoặc thiết bị bất thường cho đầu mối liên quan; ngừng thao tác theo hướng dẫn; không xóa thư, tệp, lịch sử hoặc cài lại thiết bị.

- Không đăng tải, bình luận hoặc cung cấp thông tin về sự cố khi chưa được phép; phối hợp cung cấp thiết bị, thông tin và xác nhận hoạt động nghiệp vụ khi được yêu cầu.

VII. ĐIỀU KIỆN BẢO ĐẢM, TỔ CHỨC THỰC HIỆN VÀ ĐIỀU CHỈNH, BỔ SUNG PHƯƠNG ÁN

1. Nhân lực trực triển khai và danh sách liên hệ

- Đội trưởng đội ứng cứu sự cố an ninh mạng và thành viên Đội ứng cứu sự cố duy trì phương thức liên lạc, cơ chế triệu tập theo Quy chế hoạt động; cơ quan chủ quản hệ thống thông tin quan trọng duy trì đầu mối lãnh đạo, kỹ thuật, nghiệp vụ có khả năng phản hồi ngoài giờ.

- Danh sách liên hệ ghi rõ vai trò, số điện thoại, thư điện tử, kênh bảo mật, người thay thế; được kiểm tra tối thiểu 06 tháng một lần và cập nhật ngay khi thay đổi.

- Đối với trường hợp áp dụng mức huy động lực lượng Mức 2 hoặc Mức 3, tổ chức ca trực, bàn giao, kiểm soát thời gian làm việc và quyền truy cập; mỗi ca trực phải có nhật ký, người phụ trách và nội dung bàn giao cụ thể.

2. Công cụ, hạ tầng, sao lưu và phương án dự phòng

- Bảo đảm công cụ thu thập nhật ký hệ thống, bộ nhớ, ảnh đĩa, phân tích mã độc, giám sát mạng, quản lý vụ việc, liên lạc bảo mật; thiết bị lưu trữ chuyên dụng, máy trạm sạch và môi trường phân tích cách ly.

- Duy trì hệ thống giám sát, phân tích sự kiện an ninh; giải pháp phát hiện và ứng phó trên thiết bị đầu cuối; phần mềm phòng, chống mã độc; tường lửa; tường lửa ứng dụng web; giải pháp quản lý lỗ hổng, quản lý danh tính, tài khoản đặc quyền; hệ thống sao lưu, khôi phục sau thảm họa, đồng bộ thời gian và quản lý cấu hình; bảo vệ riêng mạng quản trị và vùng sao lưu.

- Duy trì nhiều bản sao trên các loại phương tiện khác nhau, trong đó có bản sao ngoại tuyến hoặc bản sao không thể sửa đổi; định kỳ kiểm thử khả năng phục hồi; quản lý khóa mã hóa, tài khoản sao lưu và thời hạn lưu giữ độc lập với miền quản trị chính.

- Trung tâm dữ liệu và hệ thống thiết yếu có phương án nguồn điện, điều hòa, chữa cháy, đường truyền, vị trí dự phòng, thiết bị thay thế và phương án vận hành thủ công.

3. Tập huấn, diễn tập, kiểm tra và đánh giá

- Hằng năm, Công an tỉnh tham mưu Đội trưởng đội ứng cứu sự cố an ninh mạng ban hành kế hoạch hoạt động của Đội ứng cứu sự cố; chủ trì hoặc phối hợp tổ chức tập huấn, huấn luyện, diễn tập cấp tỉnh, ưu tiên tình huống có khả năng ảnh hưởng hệ thống dùng chung, dữ liệu, dịch vụ công hoặc dịch vụ thiết yếu.

- Cơ quan chủ quản hệ thống quan trọng tổ chức diễn tập phương án nội bộ, kiểm thử sao lưu, khôi phục sau thảm họa, thu hồi tài khoản, kênh liên lạc, quy

trình thủ công và truyền thông; kết quả được dùng để điều chỉnh đầu tư và hợp đồng.

- Công an tỉnh chủ trì hoặc phối hợp kiểm tra định kỳ, đột xuất; Sở Khoa học và Công nghệ kiểm tra phần hạ tầng, kết nối, vận hành và dự phòng thuộc chức năng; cơ quan chủ quản tự đánh giá tối thiểu hằng năm.

- Mọi tồn tại nguy cơ cao phải có biện pháp tạm thời, người chịu trách nhiệm và thời hạn; chậm khắc phục phải báo cáo người đứng đầu và Công an tỉnh.

4. Tổ chức thực hiện và điều chỉnh, bổ sung Phương án

- Đội trưởng đội ứng cứu sự cố an ninh mạng ban hành Quy chế hoạt động và phân công nhiệm vụ của thành viên Đội ứng cứu sự cố; Cơ quan thường trực có trách nhiệm tham mưu, theo dõi, đôn đốc, tổng hợp kết quả thực hiện và báo cáo Đội trưởng đội ứng cứu sự cố an ninh mạng, UBND tỉnh theo quy định.

- Thủ trưởng cơ quan, đơn vị, địa phương có thành viên tham gia Đội chịu trách nhiệm cử, thay thế và thông báo nhân sự; khi nhận được yêu cầu của Cơ quan thường trực hoặc Đội trưởng đội ứng cứu sự cố an ninh mạng, ưu tiên bố trí thành viên tham gia thực hiện nhiệm vụ.

- Căn cứ Phương án này và Kế hoạch số 150/KH-UBND, các cơ quan, đơn vị, địa phương ban hành hoặc cập nhật phương án nội bộ đối với từng hệ thống; gửi thông tin đầu mối và tình trạng thực hiện về Công an tỉnh theo yêu cầu.

- Phương án nội bộ phải có: tên hệ thống; chủ quản, vận hành; cấp độ; dữ liệu; kiến trúc; tài khoản; đầu mối; mục tiêu thời gian khôi phục và mục tiêu điểm khôi phục dữ liệu; sao lưu, khôi phục sau thảm họa; thao tác kỹ thuật; chế độ báo cáo; kịch bản; phương án duy trì nghiệp vụ và truyền thông.

- Công an tỉnh theo dõi, hướng dẫn, tổng hợp khó khăn, tham mưu UBND tỉnh điều chỉnh; định kỳ hằng năm và sau khi xử lý sự cố áp dụng mức huy động lực lượng Mức 3, tổ chức rà soát, đánh giá nội dung Phương án để cập nhật, bổ sung.

- Trong quá trình thực hiện, nếu có vướng mắc hoặc phát sinh tình huống chưa được quy định, cơ quan, đơn vị báo cáo Công an tỉnh để hướng dẫn theo thẩm quyền hoặc tổng hợp, tham mưu UBND tỉnh xem xét, quyết định.

Phương án này được triển khai thống nhất trên địa bàn tỉnh; các cơ quan, đơn vị, địa phương và doanh nghiệp có liên quan chịu trách nhiệm tổ chức thực hiện nghiêm túc./.