ỦY BAN NHÂN DÂN TỈNH TÂY NINH	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số: 5527/QĐ-UBND	*Tây Ninh, ngày 01 tháng 4 năm 2026*

QUYẾT ĐỊNH

Ban hành Phương án bảo vệ an toàn, an ninh thông tin và bảo mật dữ liệu khi chia sẻ giữa các sở, ngành, địa phương; Kịch bản huy động lực lượng Ứng cứu sự cố An ninh mạng trên địa bàn tỉnh

ỦY BAN NHÂN DÂN TỈNH TÂY NINH

Căn cứ Luật Tổ chức chính quyền địa phương ngày 16/6/2025;

Căn cứ Luật An toàn thông tin mạng ngày 19/11/2015;

Căn cứ Luật An ninh mạng ngày 12/6/2018;

Căn cứ Luật Bảo vệ bí mật nhà nước ngày 15/11/2018;

Căn cứ Luật Bảo vệ dữ liệu cá nhân ngày 26/6/2025;

Căn cứ Chỉ thị số 57-CT/TW ngày 31/12/2025 của Ban Bí thư về tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị;

Căn cứ Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng;

Căn cứ Quyết định số 8749/QĐ-UBND ngày 18/11/2025 của Chủ tịch UBND tỉnh về việc phân công Công an tỉnh là đơn vị chuyên trách về an toàn thông tin trên địa bàn tỉnh Tây Ninh;

Theo đề nghị của Giám đốc Công an tỉnh tại Tờ trình số 73/TTr-CAT ngày 17/3/2026.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Phương án bảo vệ an toàn, an ninh thông tin và bảo mật dữ liệu khi chia sẻ giữa các Sở, ngành, địa phương và Kịch bản huy động lực lượng Ứng cứu sự cố An ninh mạng trên địa bàn tỉnh Tây Ninh.

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

Điều 3. Thủ trưởng các Sở, ban, ngành tỉnh; Đội ứng cứu sự số an ninh mạng tỉnh Tây Ninh; Chủ tịch UBND các xã, phường chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Cục ANM và PCTP sử dụng CNC - BCA;
- TT. TU; TT. HĐND tỉnh (b/c);
- CT, các PCT. UBND tỉnh;
- CVP, các PCVP. UBND tỉnh;
- Các Sở, ban, ngành tỉnh;
- UBND các xã, phường;
- Phòng: VHXH, NC;
- Lưu: VT, th.

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

(Đã ký

Phạm Tấn Hòa

ỦY BAN NHÂN DÂN TỈNH TÂY NINH	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc

PHƯƠNG ÁN

Bảo vệ an toàn, an ninh thông tin và bảo mật dữ liệu khi chia sẻ giữa các cơ quan

(Ban hành kèm theo Quyết định số 5527 /QĐ-UBND ngày 0 tháng 4 năm 2026 của Ủy ban nhân dân tỉnh Tây Ninh)

Chương I
QUY ĐỊNH CHUNG

1. Mục tiêu

- Bảo đảm tuyệt đối an ninh, an toàn về hạ tầng thông tin, hệ thống thông tin trọng yếu và bảo mật dữ liệu khi chia sẻ giữa các cơ quan trên địa bàn tỉnh.

- Các lực lượng tham gia triển khai nhiệm vụ phải phối hợp đồng bộ, chặt chẽ nhằm phòng ngừa, ngăn chặn phát hiện sớm và xử lý kịp thời mọi sự cố an ninh mạng, hành vi tấn công mạng đối với các hệ thống thông tin trọng yếu, làm gián đoạn hệ thống hoặc rò rỉ thông tin nhạy cảm, mức độ ảnh hưởng thông tin ở diện rộng, thông tin có nội dung bí mật nhà nước trên không gian mạng.

- Quá trình triển khai thực hiện bảo đảm bố trí đầy đủ lực lượng, phương tiện, sẵn sàng xử lý hiệu quả khi có tình huống phức tạp nảy sinh.

2. Phạm vi, đối tượng

- Các cơ sở hạ tầng, hệ thống công nghệ thông tin được chia sẻ giữa các cơ quan; hệ thống thông tin các cơ quan Đảng, Nhà nước trên địa bàn tỉnh.

- Hệ thống thông tin, hệ thống mạng nội bộ BCANet, hệ thống máy chủ và lưu trữ tài liệu, hình ảnh; nền tảng truyền thông mạng xã hội (Fanpages, Livestream Facebook, Youtube, Tiktok...); Cổng/trang thông tin điện tử của Ban Tuyên giáo và Dân vận, UBND tỉnh, các Sở, ban, ngành tỉnh; màn hình điện tử tại các khu vực công cộng, có phạm vi phổ cập thông tin mức độ vừa và lớn.

3. Nguyên tắc bảo đảm an ninh mạng, an toàn thông tin

- Tuân thủ đầy đủ các văn bản quy định về việc bảo đảm an ninh mạng, an toàn thông tin; ứng phó, khắc phục sự cố an ninh mạng; quy trình, quy chế quản lý, vận hành, khai thác, sử dụng hệ thống.

- Hạ tầng kỹ thuật, trang thiết bị phải có nguồn gốc, xuất xứ rõ ràng, được kiểm tra an ninh, an toàn theo quy định.

- Triển khai các giải pháp đảm bảo an ninh mạng, an toàn thông tin và bảo mật dữ liệu khi chia sẻ trên hệ thống thông tin theo quy định; rà soát, chuẩn hóa các chính sách bảo mật cho hệ thống.

4. Phân cấp bảo vệ hệ thống mạng

4.1. Cấp tỉnh

- Lực lượng tại chỗ: Các Sở, ban, ngành, địa phương *(chủ quản hệ thống thông tin)* chịu trách nhiệm vận hành, bảo vệ các hệ thống thông tin thuộc phạm vi quản lý; cập nhật các bản vá lỗ hổng bảo mật mới nhất.

- Đơn vị vận hàng Trung tâm dữ liệu: Sở Khoa học và Công nghệ tỉnh chịu trách nhiệm bảo vệ hạ tầng Công nghệ thông tin, các hệ thống phần mềm dùng chung tại Trung tâm tích hợp dữ liệu tỉnh.

- Đơn vị giám sát: Công an tỉnh chủ trì, phối hợp các sở, ban, ngành, địa phương thực hiện công tác kiểm tra, đánh giá, điều tra, xử lý các hành vi vi phạm pháp luật về an ninh mạng, để tham mưu đề xuất có giải pháp bảo đảm an toàn thông tin kịp thời; là cơ quan thường trực của Đội Ứng cứu sự cố An ninh mạng tỉnh.

4.2. Cấp xã, phường

- Chủ động xử lý ban đầu sự cố liên quan đến cơ quan, đơn vị. Đồng thời, thông báo đến Đội Ứng cứu sự cố an ninh mạng tỉnh để phối hợp xử lý và truy vết (nếu có).

- Hàng năm rà soát các hệ thống thông tin đang quản lý, đề xuất gia hạn bản quyền các phần mềm phòng chống Virus, trang thiết bị bảo đảm an toàn thông tin theo quy mô của cơ quan, đơn vị và lập hồ sơ đề xuất cấp độ.

- Phối hợp với cơ quan cấp trên kiểm tra an toàn thông tin của cơ quan, đơn vị; thường xuyên cập nhật các bản vá lỗ hổng bảo mật mới nhất…

5. Công cụ, thiết bị

- Sử dụng thiết bị bảo mật mạng có nguồn gốc, xuất xứ rõ ràng, có độ tin cậy cao.

- Phần mềm phòng chống mã độc bản quyền có đầy đủ tính năng và khả năng cảnh báo mã độc cao nhất, có tính năng tổng quát, phân tích, đánh giá.

6. Lực lượng tham gia

- Các tổ chức, doanh nghiệp tham gia xây dựng, cung cấp hệ thống thông tin; cung cấp dịch vụ mạng viễn thông Internet...; lực lượng chuyên trách, kiêm nhiệm vận hành hệ thống thông tin, an ninh, an toàn thông tin, ứng phó và khắc phục sự cố tại chỗ của các sở, ngành và UBND các xã, phường.

- Đội Ứng cứu sự cố An ninh mạng của tỉnh (tham gia khắc phục sự cố trên địa bàn tỉnh).

Chương II
GIẢI PHÁP THỰC HIỆN

1. Phân công lực lượng bảo đảm an ninh, an toàn thông tin

- Giao Đội Ứng cứu sự cố an ninh mạng tỉnh chủ động phối hợp đơn vị chuyên trách, chủ quản các hệ thống thông tin, các đơn vị cung cấp dịch vụ viễn

thông, Internet, tiến hành giám sát lưu lượng mạng, hệ thống giám sát tập trung... để kịp thời phát hiện hoạt động tấn công mạng nhằm vào các hệ thống thông tin có chia sẻ dữ liệu giữa các cơ quan; phối hợp xử lý sự cố ban đầu, điều tra, truy vết, xác minh nguồn, nguyên nhân tấn công mạng nhằm vào hệ thống *(nếu có).*

- Giao Công an tỉnh, Sở Khoa học và Công nghệ tỉnh chủ trì phối hợp các Sở, ngành, địa phương, đơn vị chuyên trách, chủ quản các hệ thống thông tin, các đơn vị cung cấp dịch vụ viễn thông, Intermet: *(1)* Giám sát tình trạng hoạt động các thiết bị trong hệ thống; *(2)* Giám sát phát hiện tấn công từ chối dịch vụ (DDoS) vào hạ tầng cơ sở dữ liệu được chia sẻ giữa các cơ quan; *(3)* Giám sát xâm nhập mã độc vào hệ thống mạng (nếu có); *(4)* Giám sát phát hiện tấn công rà quét dịch vụ được sử dụng; *(5)* Giám sát phát hiện tấn công khai thác lỗ hổng bảo mật có liên quan đến thiết bị, ứng dụng mà hệ thống đang được sử dụng kết nối, chia sẻ dữ liệu.

2. Giải pháp bảo vệ an toàn, an ninh thông tin và bảo mật dữ liệu chia sẻ giữa các cơ quan

(1) Các Sở, ban, ngành, địa phương tăng cường công tác nghiên cứu, quán triệt, chấp hành nghiêm các chủ trương, chính sách của Đảng, pháp luật của Nhà nước về an ninh, an toàn thông tin và bảo vệ bí mật nhà nước trên không gian mạng như: Chỉ thị số 09/TTg ngày 23/02/2024 của Thủ tướng Chính phủ về tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ; Nghị định 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng; Luật số 91/2025/QH15 ngày 26/6/2025 của Quốc hội về bảo vệ dữ liệu cá nhân…

(2) Triển khai Phương án phòng chống tấn công mạng, trong đó cần nêu rõ các giải pháp ứng phó cụ thể đối với từng trường hợp tấn công mạng, cơ chế phối hợp giữa các lực lượng, đơn vị chuyên trách để chủ động phòng ngừa, ngăn chặn các hoạt động tấn công, xâm nhập vào các hệ thống mạng, Cổng/Trang thông tin điện tử nhằm phá hoại hoặc thu thập dữ liệu cá nhân, dữ liệu bí mật nhà nước của các cơ quan, đơn vị.

(3) Nâng cao chất lượng, đổi mới công tác tuyên truyền, phổ biến, đào tạo, tập huấn nâng cao trình độ, nhận thức của cán bộ, đảng viên, công chức, viên chức trên địa bàn tỉnh về công tác bảo đảm an toàn, an ninh thông tin và bảo vệ bí mật nhà nước trên không gian mạng. Trang bị cho cán bộ, đảng viên những kiến thức, kỹ năng cơ bản khi hoạt động trên môi trường mạng, việc bảo vệ dữ liệu bí mật nhà nước, dữ liệu cá nhân, những biện pháp giúp phòng ngừa các hoạt động tấn công, xâm nhập vào hệ thống mạng.

(4) Các Sở, ban, ngành, địa phương ban hành, hoàn thiện các quy chế, quy định về đảm bảo an ninh, an toàn thông tin, bảo vệ bí mật nhà nước trên không gian mạng. Trong đó, cần tập trung chấn chỉnh, sửa đổi, bổ sung những tồn tại, hạn chế, thiếu sót trong quản lý, sử dụng thiết bị, máy vi tính, mạng nội bộ, Internet như: việc sử dụng, quản lý các tài khoản, mật khẩu kết nối cơ sở dữ liệu phục vụ chuyển đổi số *(hệ thống một cửa điện tử, quản lý văn bản, các phần mềm nghiệp vụ…)*; nghiêm cấm việc kết nối máy tính soạn thảo, lưu trữ tài liệu bí mật

nhà nước vào Internet và ngược lại; tuyệt đối không sử dụng các thiết bị ngoại vi, điện thoại thông minh, USB, thiết bị lưu trữ chưa được mã hóa kết nối giữa máy tính bí mật nhà nước và máy tính kết nối mạng Internet… Nâng cao vai trò của cán bộ lãnh đạo, chỉ huy trong việc quản lý, giám sát cán bộ, đảng viên; kịp thời phát hiện các sai phạm, chấn chỉnh và xử lý theo quy định.

(5) Thực hiện công tác rà soát, thanh tra, kiểm tra thực tế, đánh giá an toàn, an ninh thông tin, kiểm tra việc chấp hành các quy định về công tác bảo vệ bí mật nhà nước trên không gian mạng của cán bộ, đảng viên tại các Sở, ban, ngành, địa phương. Kịp thời hướng dẫn, chấn chỉnh những tồn tại, hạn chế và xử lý các sai phạm theo đúng quy định.

(6) Phân công lực lượng chuyên trách về an ninh, an toàn thông tin thường xuyên rà quét, kiểm tra, đánh giá các hệ thống thông tin trên địa bàn tỉnh. Kịp thời phát hiện các điểm yếu, lỗ hổng bảo mật có nguy cơ dẫn đến mất an toàn, an ninh thông tin và thông báo đến các đơn vị vận hành hệ thống để có biện pháp khắc phục, xử lý.

(7) Chú trọng đầu tư cơ sở vật chất, trang thiết bị kỹ thuật phục vụ cho công tác đảm bảo an toàn, an ninh thông tin. Nghiên cứu đầu tư, xây dựng hệ thống giám sát, bảo vệ an ninh mạng có khả năng phát hiện, cảnh báo các hoạt động có biểu hiện nghi vấn tấn công xâm nhập, đánh cắp thông tin và các hoạt động không đúng quy định của cán bộ, công chức. Không trang bị các thiết bị, máy vi tính của các hãng công nghệ đã bị cảnh báo nguy cơ mất an toàn, an ninh thông tin. Phân công lực lượng chuyên môn chủ động rà soát, kiểm tra, đánh giá bảo mật đối với các thiết bị đã được trang bị nhưng chưa qua kiểm tra và thực hiện rà quét, đánh giá bảo mật đối với từng thiết bị mới trước khi đưa vào sử dụng.

(8) Chú trọng công tác đào tạo, nâng cao trình độ, năng lực cho đội ngũ chuyên trách về công tác đảm bảo an toàn, an ninh mạng. Thường xuyên phối hợp, liên kết với các đơn vị nghiệp vụ của Bộ Khoa học và Công nghệ, các tổ chức, doanh nghiệp, chuyên gia an ninh mạng tổ chức nhiều đợt tập huấn chuyên sâu về kỹ năng, phát triển nhiều giải pháp cho lực lượng, Đội Ứng cứu sự cố an toàn thông tin của tỉnh; kịp thời phối hợp, hỗ trợ khi xảy ra các sự cố tấn công mạng trên địa bàn tỉnh.

(9) Tổ chức diễn tập thực chiến định kỳ. Công an tỉnh chủ trì, phối hợp với Sở Khoa học và Công nghệ tỉnh và các đơn vị liên quan xây dựng kịch bản, tổ chức diễn tập ứng cứu sự cố an ninh mạng hằng năm cho Đội ứng cứu sự cố An ninh mạng tỉnh và các lực lượng chuyên trách. Lựa chọn hệ thống thông tin có nguy cơ cao xảy ra các cuộc tấn công mạng, tập trung vào các mã độc nguy hiểm nhất hiện nay như mã độc tống tiền (Ransomware)…, khai thác lỗ hổng của các ứng dụng đã được triển khai phục vụ công tác chuyên môn nghiệp vụ nhằm đánh giá quy trình phối hợp và nâng cao năng lực phản ứng.

Chương III
TỔ CHỨC THỰC HIỆN

1. Trách nhiệm các Sở, ngành, địa phương

Thủ trưởng các Sở, ngành, địa phương tổ chức thực hiện nghiêm túc, có hiệu quả các giải pháp bảo vệ an toàn, an ninh thông tin và bảo mật dữ liệu khi chia sẻ giữa các cơ quan; cử đầu mối phối hợp thực hiện trong trường hợp phát hiện sự cố mất an ninh, an toàn thông tin.

2. Trách nhiệm của Công an tỉnh

Công an tỉnh chủ trì phối hợp với Sở Khoa học và Công nghệ tỉnh và các cơ quan chủ quản hệ thống thông tin hướng dẫn, đôn đốc, kiểm tra việc triển khai, thực hiện Phương án, hằng năm có báo cáo đánh giá, rút kinh nghiệm, đề xuất bổ sung, hoàn thiện Phương án theo tình hình thực tế./.

ỦY BAN NHÂN DÂN
TỈNH TÂY NINH

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

KỊCH BẢN HUY ĐỘNG LỰC LƯỢNG, ỨNG CỨU SỰ CỐ AN NINH MẠNG

(Ban hành kèm theo Quyết định số 5527/QĐ-UBND ngày 01 tháng 4 năm 2026 của Ủy ban nhân dân tỉnh Tây Ninh)

1. Kịch bản xử lý một số tình huống tấn công mạng và biện pháp xử lý bảo đảm an ninh mạng, an toàn thông tin

1.1. Xử lý tình huống chung

Bước 1. Nhận diện sự cố: Phát hiện dấu hiệu bất thường từ hệ thống thông tin, người dùng hoặc cảnh báo từ các công cụ, thiết bị bảo mật (IPS/IDS, SIEM, Firewall, Antivirus...); ghi lại thông tin sự cố như: thời gian, dấu hiệu, hệ thống bị ảnh hưởng, người phát hiện; báo cáo cấp có thẩm quyền để thực hiện các bước tiếp theo.

Bước 2. Đánh giá và phân loại: Xác định loại sự cố đó là do phần mềm độc hại, tấn công từ chối dịch vụ (DDoS), tấn công phishing, rò rỉ dữ liệu, tấn công - bruteforce…; đánh giá mức độ nghiêm trọng theo các mức: thấp, trung bình, cao, nghiêm trọng, đặc biệt nghiêm trọng.

Bước 3. Cô lập và ngăn chặn: Tùy từng mức độ nghiêm trọng mà có thể ngắt kết nối thiết bị ra khỏi hệ thống mạng; chặn IP nguồn tấn công; vô hiệu hóa tài khoản bị xâm nhập.

Bước 4. Xử lý và khôi phục: Gỡ bỏ mã độc, vá lỗ hổng bảo mật; khôi phục hệ thống từ bản sao lưu sạch gần nhất; thay đổi thông tin đăng nhập bị rò rỉ; khôi phục dịch vụ và kiểm tra hoạt động.

Bước 5. Điều tra xác minh và phân tích: Phân tích lịch sử logs, tìm nguồn gốc cuộc tấn công; xác định cách thức của đối tượng tấn công xâm nhập; thu thập chứng cứ số, bằng chứng điện tử.

Bước 6. Báo cáo và khắc phục: Báo cáo chi tiết về sự cố, hậu quả và cách xử lý; nhận xét, đề xuất và cập nhật chính sách bảo mật; phổ biến, hướng dẫn lại đơn vị chủ trì vận hành hệ thống thông tin nếu cần thiết.

1.2. Một số tình huống cụ thể và cách xử lý

- Tấn công từ chối dịch vụ DDoS: Cô lập hệ thống bằng Firewall hoặc sử dụng dịch vụ chống DDoS để lọc traffic; giới hạn truy cập, ưu tiên các dịch vụ quan trọng; xác định IP nguồn và loại hình tấn công là SYN flood hay UDP flood..; liên hệ nhà cung cấp dịch vụ ISP bổ sung băng thông nếu cần thiết.

- Máy tính bị nhiễm virus, mã độc, phần mềm độc hại: Xử lý bằng cách ngắt kết nối mạng để ngăn lan truyền qua máy tính khác; khởi động máy vào chế độ SafeMode; quét virus bằng phần mềm Antivirus bản quyền; gỡ phần mềm lạ, đáng ngờ; cân nhắc cài đặt lại hệ điều hành (chú ý sao lưu dữ liệu quan trọng) nếu các công cụ Antivirus không loại bỏ được hết malware, ransomeware..

- ***Bị tấn công Phishing:*** Tin tặc thường gửi Email, SMS, tin nhắn messenger, zalo, facebook có đường link lạ giống như thật nhưng có sai khác nhỏ (***ví dụ như https://dichvucongn.gov.vn*** thay vì ***https://dichvucong.gov.vn***), chúng yêu cầu nạn nhân đăng nhập thông tin cá nhân, yêu cầu thông tin tài khoản/mật khẩu, mã OTP bất thường.

Cách xử lý: Không nhập vào đường link lạ hoặc tải tệp đính kèm, không trả lời tin nhắn, email đáng nghi; nêu đã lỡ nhấp vào đường link hoặc tải tệp tin đính kèm thì lập tức ngắt kết nối internet, chạy chương trình Antivirus, sau đó đổi mật khẩu của tài khoản bị xâm nhập và tài khoản khác dùng chung mật khẩu đó, kích hoạt xác thực hai yếu tố để tăng cường bảo mật.

- ***Hệ thống bị tấn công qua lỗ hổng ứng dụng, website:*** Cách nhận biết hệ thông bị tấn công mạng: lưu lượng truy cập tăng đột biến bất thường, website phản hồi chậm, xuất hiện dữ liệu lạ trong cơ sở dữ liệu, các hành vi bất thường trong log SQL Injection, xss payloads, brute-force login...

Cách xử lý: Chặn IP tấn công qua firewall hoặc WAF, cập nhật các rule WAF để chặn payload tấn công, rollback hệ thống về bản backup an toàn nếu có thể, cập nhật code và thư viện lên phiên bản cao nhất, cập nhật framework/CMS, kiểm tra định kỳ và backup dữ liệu thường xuyên.

- ***Trang, cổng thông tin điện tử bị tấn công thay đổi giao diện****:* Để hạn chế thiệt hại, rủi ro khi bị tấn công deface, quản trị hệ thống phải ngắt kết nối internet hoặc chuyển hướng sang chế độ bảo trì để ngăn chặn tin tặc tiếp tục khai thác, cần thiết chuyển server về chế độ chỉ đọc; sau đó ghi nhận logfile của web server, hệ điều hành, firewall; phân tích nguyên nhân, kiểm tra lỗ hổng bảo mật (SQL injection, xss, uploadfile, plugin cũ..), xem xét đến khả năng tài khoản quản trị bị lộ, phần mềm hệ thống hoặc CMS có lỗ hổng, có shell/backdoor bị cài...; sau đó khôi phục hệ thống, tăng cường bảo mật bằng các cách như: đổi toàn bộ mật khẩu (FTP, SSH. CMS, DB..), cài đặt và cấu hình lại WAF, hạn chế quyền truy cập, cập nhật các bản vá bảo mật mới nhất, tắt hoặc giới hạn các chức năng upload, thực thi mã.

- ***Tài khoản bị xâm nhập:*** Quản trị hệ thống lập tức khóa tạm thời tài khoản bị xâm nhập; thu hồi tất cả token đăng nhập; chặn IP bất thường; đăng xuất toàn bộ phiên đăng nhập; kiểm tra nguyên nhân bị xâm nhập từ đó có thể đặt lại "mật khẩu" và yêu cầu người dùng xác nhận lại danh tính, đổi mật khẩu định kỳ, xác

thực hai yếu tố, giới hạn IP hoặc vị trí địa lý cho tài khoản admin, cảnh báo đăng nhập bất thường.

- ***Khi màn hình quảng cáo bị tấn công chèn nội dung, hình ảnh trái phép:*** Lập tức ngắt nguồn điện hoặc ngắt kết nối mạng để dừng nội dung hình ảnh bị chèn; lập biên bản sự cố, ghi nhận hình ảnh lại làm bằng chứng, ghi nhận thông tin, thời gian xảy ra sự cố; kiểm tra và ngắt các kết nối không cần thiết (wifi, NFC, Bluetooth); kiểm tra các Port điều khiển từ xa qua internet có bị mở hay không (3389, 8080); kiểm tra thiết bị xem có bị kết nối từ xa qua VNC, AnyDesk, Teamviewer, Ultraview, RemoteDesktop, Seecreen..; gỡ toàn bộ phần mềm điều khiển cũ, cài lại phiên bản mới và sạch; đổi mật khẩu truy cập thiết bị; tắt quyền truy cập từ xa nếu thấy không cần thiết.

2. Huy động lực lượng ứng cứu sự cố hoạt động tấn công mạng, bảo đảm an toàn thông tin các hệ thống

Tổ trưởng Tổ ứng cứu sự cố an ninh mạng của tỉnh căn cứ tình hình thực tế huy động thành viên và cán bộ chuyên trách an toàn thông tin tại các sở, ngành và UBND các xã, phường tham gia xử lý sự cố./.