BỘ CÔNG AN
CÔNG AN TỈNH BẮC NINH

Số: 672/CAT-ANM

V/v triển khai phương án bảo đảm an ninh, an toàn thông tin và ứng cứu sự cố an ninh mạng phục vụ bầu cử đại biểu Quốc hội khóa XVI và đại biểu Hội đồng nhân dân các cấp nhiệm kỳ 2026-2031

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

Bắc Ninh, ngày 01 tháng 02 năm 2026

Kính gửi:
- Các ban, cơ quan thuộc Tỉnh ủy;
- Uỷ ban MTTQ tỉnh;
- Các sở, cơ quan trực thuộc UBND tỉnh;
- Các cơ quan trung ương trên địa bàn tỉnh;
- Cơ quan báo chí, đài phát thanh, truyền hình, cơ quan thông tấn trên địa bàn tỉnh;
- Chi nhánh doanh nghiệp viễn thông trên địa bàn tỉnh;
- UBND các xã, phường.

Bầu cử đại biểu Quốc hội khóa XVI và đại biểu Hội đồng nhân dân các cấp nhiệm kỳ 2026 – 2031 (sau đây gọi chung là "cuộc bầu cử") được triển khai, tổ chức trên toàn quốc vào ngày Chủ nhật (15/3/2026) là sự kiện chính trị quan trọng của đất nước, là dịp để mỗi người dân trực tiếp thể hiện quyền làm chủ, thể hiện ý chí và trách nhiệm đối với sự phát triển của đất nước. Thực hiện Kế hoạch số 24/KH-TBANTT ngày 14/01/2026 của Tiểu ban an ninh, trật tự cuộc bầu cử; Chỉ thị số 06/CT-UBND ngày 09/12/2025 của UBND tỉnh về thực hiện đợt Cao điểm tấn công, trấn áp tội phạm, bảo đảm an ninh trật tự Đại hội đại biểu toàn quốc lần thứ XIV, bầu cử đại biểu Quốc hội khoá XVI, Hội đồng nhân dân các cấp nhiệm kỳ 2026 - 2031, Tết Nguyên đán Bính Ngọ 2026, các sự kiện lớn của đất nước, địa phương và các lễ hội đầu năm. Nhằm đảm bảo an ninh, an toàn thông tin và ứng cứu sự cố an ninh mạng phục vụ cuộc bầu cử, Công an tỉnh đề nghị các cơ quan, đơn vị, doanh nghiệp có liên quan tổ chức thực hiện các nội dung sau:

1. Triển khai phương án đảm bảo an ninh, an toàn thông tin và ứng cứu sự cố an ninh mạng đối với hệ thống thông tin đang quản lý, vận hành *(có phương án kèm theo).*

2. Tăng cường công tác đảm bảo an ninh, an toàn thông tin đối với trang thiết bị triển khai tại các địa điểm bầu cử cấp tỉnh, xã, phường bao gồm: Hệ thống mạng nội bộ LAN/VLAN, Wifi, các thiết bị đầu cuối (máy tính, thiết bị tác nghiệp), hệ thống thu phát sóng, truyền thanh, truyền hình trực tiếp, thiết bị sân khấu, hội trường, màn hình LED, pano, áp phích điện tử… phục vụ bầu cử.

3. Đẩy mạnh tuyên truyền, phổ biến, giáo dục pháp luật về bảo đảm an ninh mạng, an toàn thông tin, bảo vệ BMNN trong nội bộ các cơ quan, đơn vị, doanh nghiệp; đồng thời, đẩy mạnh tuyên truyền về công tác bảo đảm an ninh mạng, an toàn thông tin trên trang thông tin điện tử, trang mạng xã hội và các phương tiện thông tin đại chúng phổ biến nhằm nâng cao nhận thức, trách nhiệm của mỗi cán bộ, công chức, viên chức, người lao động và nhân dân trên địa bàn về ý nghĩa, tầm quan trọng với công tác này.

4. Trong quá trình thực hiện nếu có thông tin cần trao đổi, các cơ quan, đơn vị, doanh nghiệp liên hệ với Công an tỉnh *(qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, đồng chí Trung tá Vũ Anh Đức, Phó trưởng phòng, SĐT: 0982.072.102)* để được hướng dẫn./.

Nơi nhận:
- Như trên;
- Bộ Công an (Cục ANM&PCTPSDCNC);
- Đ/c Bí thư Tỉnh ủy (để b/cáo);
- Đ/c Chủ tịch UBND tỉnh;
- Đ/c Chủ tịch HĐND tỉnh;
- Đ/c Giám đốc CAT;
- Lưu: VT, ANM (ATTT).

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CÔNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
CÔNG AN TỈNH BẮC NINH

Đại tá Đỗ Đức Trịnh

PHƯƠNG ÁN

Bảo đảm an ninh, an toàn thông tin và ứng cứu sự cố an ninh mạng phục vụ bầu cử đại biểu Quốc hội khóa XVI và đại biểu Hội đồng nhân dân các cấp nhiệm kỳ 2026-2031

(Kèm theo Công văn số 672/CAT-ANM ngày 01/02/2026 của Công an tỉnh)

I. QUY ĐỊNH CHUNG

1. Phạm vi, đối tượng áp dụng

- *Phạm vi:* Các cơ quan Đảng, Nhà nước, tổ chức chính trị, cơ quan, doanh nghiệp liên quan đến công tác đảm bảo an toàn thông tin mạng (ATTTM) trên địa bàn tỉnh.

- *Đối tượng:* Phương án này áp dụng đối với các hệ thống thông tin trên địa bàn tỉnh; trang/cổng thông tin của các đài phát thanh, truyền hình, cơ quan thông tấn báo chí trong và ngoài nước triển khai tại các địa điểm bầu cử cấp tỉnh, xã, phường, bao gồm: Hệ thống mạng nội bộ LAN/VLAN, Wifi, hệ thống máy chủ (web, lưu trữ, CSDL), hệ thống kiểm soát truy cập, tường lửa, IPS/ IDS, SIEM/SOC, các thiết bị đầu cuối (máy tính, thiết bị tác nghiệp), hệ thống thu phát sóng, truyền thanh, truyền hình trực tiếp, thiết bị sân khấu, hội trường; màn hình LED, pano, áp phích điện tử phục vụ bầu cử.

2. 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 ATTTM; quy trình, quy chế quản lý, vận hành, khai thác, sử dụng hệ thống.

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

- Triển khai các giải pháp, phương án đảm bảo an ninh mạng, an toàn thông tin cho hệ thống thông tin theo quy định; rà soát, chuẩn hóa các chính sách bảo mật cho hệ thống.

II. PHÂN LOẠI SỰ CỐ AN NINH MẠNG

1. Phân loại theo tính chất tấn công

- *Tấn công từ chối dịch vụ (DDos):* Làm gián đoạn hoặc tê liệt hoạt động của trang/cổng thông tin điện tử phục vụ cuộc bầu cử, các dịch vụ, máy chủ hệ thống thông tin bằng cách làm ngập hệ thống với lưu lượng truy cập quá mức từ nhiều nguồn khác nhau.

- *Tấn công thay đổi giao diện (Deface):* Tin tặc xâm nhập hệ thống quản trị trang/cổng thông tin điện tử, màn hình LED, bảng điện tử, pano, áp - phích tuyên truyền để lại thông điệp chính trị, nội dung xấu độc, đe dọa hoặc video- hình ảnh không đúng thuần phong mỹ tục...

- *Tấn công chèn mã độc (Malware, Ransomeware):* Tin tặc xâm nhập hệ thống thông tin và cài đặt phần mềm độc hại nhằm đánh cắp thông tin, BMNN, phá hoại hệ thống, gián điệp hoặc tống tiền.

- *Tấn công có chủ đích (APT):* Là một dạng tấn công có tổ chức, kéo dài, được lên kế hoạch kỹ lưỡng, nhằm xâm nhập hệ thống mạng của Quốc hội và Hội đồng nhân dân (HĐND) các cấp để kiểm soát, theo dõi, đánh cắp thông tin một cách bí mật, lâu dài mà không phát hiện ra bằng cách thông thường.

- *Tấn công lừa đảo (Phishing):* Giả mạo thông tin, danh tính (email, website, tài liệu, tin nhắn...) để lừa người dùng cung cấp thông tin nhạy cảm như tài khoản truy cập, mật khẩu, mã OTP, tài liệu nội bộ, hoặc vô tình bấm vào đường link để cài đặt phần mềm, mã độc.

- *Tấn công qua mạng xã hội, truyền thông (Fake news, botnet):* Lợi dụng nền tảng facebook, X (Twitter), Youtube, Tiktok, Zalo... để phát tán mã độc, lừa đảo, mạo danh tính, phát tán thông tin sai lệch nhằm gây rối loạn thông tin, làm giảm uy tín lãnh đạo, can thiệp dư luận, làm lộ thông tin bí mật đời tư, định hướng sai dư luận xã hội, rối loạn truyền thông, gây chia rẽ nội bộ, tung danh sách cán bộ, nhà báo...

2. Phân loại theo mức độ nghiêm trọng

- *Nghiêm trọng mức I (mức cao):* Là loại sự cố gây gián đoạn hoàn toàn hoặc làm tê liệt hệ thống thông tin quan trọng, gây rò rỉ thông tin cử tri, hoặc dẫn đến mất quyền kiểm soát hệ thống, ảnh hưởng trực tiếp đến ANQG và hoạt động điều hành của Ban Tổ chức. Tình huống có thể là: Danh sách cử tri, thông tin cử tri, kết quả bầu cử không chính xác bị đưa công khai lên mạng xã hội, internet; Trang thông tin chính thức của HĐND các cấp bị thay đổi giao diện, xuất hiện thông tin phản động, xuyên tạc đường lối chính sách của Đảng, Nhà nước...

- *Nghiêm trọng mức II (mức trung bình):* Là sự cố gây ảnh hưởng đến một phần hệ thống hoặc một nhóm người dùng, làm gián đoạn tạm thời các hoạt động, ảnh hưởng đến tính sẵn sàng hoặc độ tin cậy của hệ thống thông tin nhưng không gây ra hậu quả nghiêm trọng đến hệ thống điều hành, không làm lộ, mất BMNN. Ví dụ: hệ thống bị tấn công rò quét mật khẩu, thăm dò; trang thông tin điện tử Đoàn đại biểu Quốc hội và HĐND tỉnh không thể cập nhật thông tin trong thời gian ngắn; màn hình điện tử bị treo logo hoặc nhấp nháy; máy tính phục vụ cuộc bầu cử chưa được kiểm tra an ninh, an toàn bị nhiễm virus, mã độc...

- *Nghiêm trọng mức III (mức thấp):* Là sự cố nhỏ không gây gián đoạn dịch vụ, hệ thống mạng, không xâm nhập vào hệ thống quan trọng, không làm mất dữ liệu nhưng tiềm ẩn nhiều nguy cơ nếu không được xử lý kịp thời. Sự cố nhỏ thường là các sự cố ở thiết bị cá nhân, thiết bị đầu cuối, các biểu hiện spam, xâm nhập không thành công, dò đoán mật khẩu, nghi ngờ email, tin nhắn rác...

3. Phân loại theo đối tượng bị ảnh hưởng

- Hạ tầng mạng, hệ thống thông tin trên địa bàn tỉnh.

- Hạ tầng mạng, hệ thống truyền thông của cơ quan thông tấn báo chí triển khai trên địa bàn tỉnh.

- Hạ tầng mạng, hệ thống truyền hình, truyền thanh trực tiếp trên địa bàn tỉnh.

- Các thiết bị đầu cuối, người dùng cuối (endpoint): Máy tính, điện thoại, tablet,

máy ghi hình, camera, điện thoại VoIP, thiết bị video conference, thiết bị IoT...

- Hệ thống tuyên truyền, truyền thông đại chúng: Smart tivi, màn hình LED, bảng điện tử, Fanpage chính thức của HĐND các cấp, trang báo điện tử, các nền tảng số (app, OTT, web)…

III. QUY TRÌNH ỨNG ỨNG CỨU SỰ CỐ

1. Phát hiện sự cố

- Phát hiện sớm các cuộc tấn công mạng hoặc sự cố an toàn thông tin mạng; khoanh vùng nhanh, tránh để lan rộng, gây ảnh hưởng đến toàn bộ hệ thống thông tin; hệ thống cảnh báo tự động giúp xử lý sự cố an toàn thông tin sớm nhất có thể.

- Phát hiện bằng các phương thức giám sát tự động, sử dụng công cụ kỹ thuật phát hiện bất thường IDS/IPS, SIEM/SOC, Filewall logs, Endpoint Security/EDR, giám sát lưu lượng mạng, hoặc phát hiện sự cố qua thiết bị đầu cuối của người dùng, đại biểu...

2. Xác định và đánh giá sự cố

Tổ trưởng tổ ứng cứu sự cố xác nhận và kiểm tra cảnh báo có đúng là sự cố thực sự hay không, hay chỉ là cảnh báo giả (False alarm) do hệ thống phát hiện nhầm hoặc thao tác sai của người dùng; đánh giá mức độ nghiêm trọng của sự cố theo mức độ thấp, trung bình, cao, nghiêm trọng để đưa ra quyết định xử lý ban đầu; dựa vào kết quả đánh giá sẽ quyết định cô lập một số thành phần của hệ thống thông tin, triển khai ứng cứu toàn diện hay có cần báo cho cấp trên để được hướng dẫn, chỉ đạo.

3. Cô lập, khoanh vùng sự cố an ninh mạng

Đây là giai đoạn then chốt giúp ngăn chặn sự cố lan rộng và kiểm soát phạm vi ảnh hưởng đến toàn bộ hệ thống thông tin như ngăn chặn lây lan của mã độc, truy cập trái phép dữ liệu; giữ ổn định hệ thống còn lại để có điều kiện phân tích, xử lý sự cố an toàn; cần cô lập, khoanh vùng khi phát hiện máy chủ, thiết bị, tài khoản có dấu hiệu bị xâm nhập, phát hiện mã độc có hành vi bất thường trong hệ thống, website bị tấn công thay đổi giao diện, thay đổi nội dung trái phép...; cô lập ở cấp độ mạng như chặn IP, miền (domain) đang tấn công, tạm thời tắt các VLAN, subnet hoặc ngắt thiết bị nghi ngờ; chuyển hướng lưu lượng mạng qua hệ thống lọc (WAF, Anti-DDoS) để cô lập gói tin độc hại; cô lập ở cấp độ tài khoản; cô lập logic trong phần mềm, hệ thống.

4. Phân tích, xử lý

- Thu thập dữ liệu, chứng cứ số từ filewall, máy chủ, thiết bị đầu cuối, hệ điều hành, ứng dụng...sau đó sử dụng các công cụ phân tích log, phân tích gói tin mạng bằng các công cụ ELK Stack, FTK Image, Autopsy, Wireshark; xác định nguyên nhân gốc như lỗ hổng bảo mật chưa được vá, mật khẩu yếu, cấu hình sai, thiết bị đầu cuối bị cài mã độc, tài khoản nội bộ bị đánh cắp...

- Xử lý sự cố qua các hình thức xóa bỏ mã độc, vá lỗ hổng hệ điều hành, phần mềm ứng dụng; đổi mật khẩu toàn hệ thống, nhất là tài khoản quản trị; tăng cường phân quyền, xác thực đa yếu tố; tắt các dịch vụ không cần thiết, đóng cổng

mạng không dùng đến...; kiểm tra kỹ lưỡng khi đưa hệ thống hoạt động trở lại.

5. Khôi phục và theo dõi

Đưa hệ thống trở lại trạng thái an toàn, ổn định, hoạt động bình thường bảo đảm không còn mã độc, cửa hậu, không còn nguy cơ bị tấn công tiếp; khôi phục dữ liệu, dịch vụ và kết nối thông tin báo chí, truyền thông, website, truyền hình trực tiếp. Các bước khôi phục cụ thể gồm: (1) Kiểm tra toàn bộ hệ thống, diệt mã độc, xóa hoặc thay thế những thành phần bị hỏng, lỗi; (2) Khôi phục dữ liệu từ bản sao lưu gần nhất nhưng an toàn, không bị nhiễm mã độc như VM snapshot, system image..; (3) Cấu hình lại hệ thống và kiểm tra an toàn: cập nhật bản vá, đổi toàn bộ mật khẩu hệ thống, cấu hình lại Firewall, WAF, phân quyền thư mục tài khoản người dùng; (4) Vận hành, kiểm thử các dịch vụ chính như Website, truyền hình trực tuyến, livestream, hệ thống đăng ký đại biểu, tra cứu thông tin, file server...Test mạng nội bộ, kết nối các thiết bị đầu cuối, wifi, máy in, camera. Giám sát thời gian thực sau khi khôi phục; (5) Đưa hệ thống thông tin hoạt động trở lại, đối với trang/cổng thông tin điện tử cần gỡ chế độ bảo trì, gửi thông báo đến các bộ phận liên quan, mở lại truy cập cho người dùng, phóng viên, đại biểu, ban tổ chức.

6. Báo cáo, tổng kết, rút kinh nghiệm

Báo cáo về sự cố an toàn thông tin mạng phục vụ cuộc bầu cử cần phải nêu rõ đầy đủ các thông tin về sự cố, diễn biến, nguyên nhân, biện pháp đã triển khai ứng cứu sự cố, đánh giá ảnh hưởng tác động đến hoạt động truyền thông, thiệt hại về dữ liệu, mức độ sự cố, nếu không xử lý kịp thời có thể ảnh hưởng như thế nào đến uy tín của ban tổ chức sự kiện. Từ đó, rút kinh nghiệm và kiến nghị đề xuất trong thời gian tới.

IV. MỘT SỐ SỰ CỐ CỤ THỂ VÀ HƯỚNG XỬ LÝ BAN ĐẦU

1. Trang thông tin điện tử Đoàn đại biểu Quốc hội tỉnh và HĐND các cấp bị tấn công từ chối dịch vụ DDoS

- *Cách nhận biết:* Trang thông tin điện tử của tỉnh chậm bất thường hoặc không thể truy cập, thời gian tải trang tăng đột ngột, trình duyệt báo lỗi Gateway timeout, Service Unavailable (503)...; lưu lượng truy cập tăng đột biến, số lượng request tới server tăng bất thường; tài nguyên máy chủ bị sử dụng quá mức; sự cố không theo quy luật bình thường, có một số dịch vụ trên web hoạt động, có dịch vụ thì không...

- *Hướng xử lý:* Đơn vị vận hành, lập tức 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 thấy cần thiết.

2. Máy tính phục vụ cuộc bầu cử bị nhiễm virus, mã độc, phần mềm độc hại

- *Cách nhận biết:* Máy tính chạy chậm bất thường; thời gian khởi động máy tính kéo dài hơn bình thường; các ứng dụng bị treo, đơ hoặc tự động tắt mà không

rõ lý do; Pop-up quảng cáo xuất hiện liên tục, kể cả không truy cập trình duyệt; trình duyệt bị chuyển hướng đến các trang web lạ; biểu tượng (icon) phần mềm, file, thư mục bị thay đổi, mất hoặc xuất hiện file lạ...

- *Hướng xử lý:* 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…

3. Bị tấn công Phishing

- *Cách nhận biết:* 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 bacninhgov.com thay vì bacninh.gov.vn), chúng yêu cầu người dùng đăng nhập thông tin cá nhân, yêu cầu thông tin tài khoản/mật khẩu, mã OTP bất thường.

- *Hướng xử lý:* Hướng dẫn, tuyên truyền người dùng, không nhấp vào đường link hoặc tải tệp đính kèm, không trả lời tin nhắn, email đáng nghi; nếu đã lỡ nhấp vào đường link hoặc tải tệp tin đính kèm thì lập tức ngắt kết nối internet, xóa lịch sử, cookie, cache trong trình duyệt, chạy chương trình antivirus, gỡ bỏ ứng dụng lạ, khởi động lại máy (nếu dùng iPhone); nếu đã nhập thông tin vào đường link lạ thì ngay lập tức 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; trường hợp đã lỡ nhập thông tin ngân hàng vào đường dẫn lạ thì phải gọi ngay cho tổng đài ngân hàng yêu cầu khóa tài khoản, thẻ, tắt internet banking tạm thời, đổi mật khẩu, kiểm tra biến động số dư.

4. Hệ thống thông tin bị tấn công qua lỗ hổng ứng dụng, website

- *Cách nhận biết hệ thống 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...

- *Hướng 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 và an toàn, cập nhật framework/CMS, kiểm tra định kỳ và backup dữ liệu thường xuyên.

5. Trang, cổng thông tin điện tử bị tấn công thay đổi giao diện

- *Cách nhận biết:* Trên giao diện website bị chèn ký tự, thông điệp của tin tặc (deface), xuất hiện hình ảnh lạ, nội dung phản cảm...

- *Hướng xử lý:* Để hạn chế thiệt hại, rủi ro khi bị tấn công deface, quản trị hệ thống phải ngắt kết nối internet hoặc chuyển hướng website sang chế độ bảo trì để ngăn chặn tin tặc tiếp tục khai thác, cần thiết chuyển server về chế độ bảo trì; 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.

6. Khi màn hình LED, LCD, pano số, áp phích điện tử bị tấn công chèn nội dung, hình ảnh trái phép

- *Cách nhận biết:* Nội dung hiển thị bị thay đổi mà không có ai điều khiển, tự động hiện ra video, hình ảnh lạ, nội dung phản cảm, quảng cáo trá hình, cờ bạc, thông điệp chính trị, màn hình nháy, bị bật tắt hoặc reset bất thường...

- *Hướng xử lý:* Lập tức ngắt nguồn điện, hoặc ngắt kết nối mạng, tắt bộ điều khiển (controller) để dừng nội dung hình ảnh bị chèn; lập biên bản sự cố trình bày đầy đủ thông tin, 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.