BỘ CÔNG AN
CÔNG AN TỈNH QUẢNG NGÃI

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

Số: 193 /CAT-TM(ANM)

Quảng Ngãi, ngày 12 tháng 01 năm 2026

V/v bảo đảm an toàn thông tin, an ninh mạng phục vụ Đại hội đại biểu toàn quốc lần thứ XIV của Đảng

HỎA TỐC

Kính gửi:
- Ủy ban Mặt trận Tổ quốc Việt Nam tỉnh;
- Văn phòng Tỉnh ủy, UBND tỉnh;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Bộ Chỉ huy Quân sự tỉnh; Tòa án nhân dân tỉnh;
- Viện Kiểm sát nhân dân tỉnh; Thi hành án dân sự tỉnh;
- Bảo hiểm xã hội tỉnh; Cảng vụ Hàng hải Quảng Ngãi;
- Thống kê tỉnh; Thuế tỉnh Quảng Ngãi;
- Kho bạc Nhà nước khu vực XV;
- Báo và Phát thanh, Truyền hình tỉnh;
- Các sở, ban, ngành và hội đoàn thể tỉnh;
- UBND các xã, phường, đặc khu Lý Sơn;
- Trường Đại học Phạm Văn Đồng, Cao đẳng Cộng đồng Kon Tum, Cao đẳng Việt Nam - Hàn Quốc - Quảng Ngãi;
- Công ty CP lọc hóa dầu Bình Sơn; Truyền tải điện Quảng Ngãi; Điện lực Quảng Ngãi;
- Viettel Quảng Ngãi, VNPT Quảng Ngãi, Mobifone Quảng Ngãi, FPT Quảng Ngãi, SCTV Quảng Ngãi.

Nhằm tăng cường công tác bảo đảm an toàn thông tin, an ninh mạng trên địa bàn tỉnh Quảng Ngãi phục vụ Đại hội đại biểu toàn quốc lần thứ XIV của Đảng *(gọi tắt là Đại hội)*, đề nghị cơ quan, đơn vị, địa phương tập trung triển khai các nội dung sau:

1. Tăng cường bảo đảm an toàn thông tin, an ninh mạng đối với các hệ thống thông tin phục vụ Đại hội

- Triển khai thực hiện hiệu quả Công văn số 2705/CAT-TM(ANM) ngày 09/10/2025 của Công an tỉnh về bảo đảm an ninh mạng, an toàn thông tin cho Cổng thông tin điện tử phục vụ Đại hội; tăng cường công tác bảo đảm an toàn thông tin, an ninh mạng trước, trong và sau thời gian diễn ra Đại hội.

- Rà soát toàn bộ các hệ thống thông tin phục vụ công tác chỉ đạo, điều hành, tuyên truyền và tổ chức Đại hội; bảo đảm các hệ thống được triển khai đầy đủ biện pháp bảo vệ theo cấp độ an toàn thông tin đã được phê duyệt; kiểm tra, cấu hình, cập nhật các chính sách an ninh đối với hệ thống tường lửa, hệ thống phát hiện và ngăn chặn xâm nhập, hệ thống phòng, chống mã độc; kịp thời cập nhật hệ điều hành máy chủ, ứng dụng, dịch vụ và các thành phần hạ tầng công nghệ thông tin liên quan.

- Phân công lực lượng kỹ thuật tại chỗ trực, giám sát hệ thống 24/7 trước, trong và sau Đại hội, các ngày nghỉ lễ liên quan; bảo đảm duy trì hoạt động giám sát liên tục, không để xảy ra gián đoạn; theo dõi, phân tích cảnh báo từ hệ thống giám sát an toàn thông tin tập trung, hệ thống phòng, chống mã độc tập trung nhằm kịp thời phát hiện, xử lý, khắc phục nguy cơ, sự cố mất an toàn thông tin, hành vi tấn công mạng đã được xác minh.

- Kiểm tra, đánh giá an toàn thông tin đối với các hệ thống thông tin; phát hiện, khắc phục kịp thời lỗ hổng, điểm yếu bảo mật; thực hiện hoạt động săn lùng mối nguy hại, rà soát, bóc gỡ phần mềm độc hại đối với toàn bộ máy chủ, máy trạm trong hệ thống mạng; ưu tiên kiểm tra, xử lý đối với hệ thống thông tin có địa chỉ IP nằm trong danh sách IP thuộc mạng Botnet do các đơn vị chức năng cảnh báo; rà soát, cập nhật đầy đủ bản vá bảo mật cho hệ thống thông tin.

- Tuyên truyền, phổ biến, nâng cao nhận thức và trang bị kỹ năng cơ bản về an toàn thông tin mạng; nâng cao tinh thần cảnh giác đối với thông tin xấu độc, tin giả, thông tin sai sự thật và hành vi lừa đảo trên không gian mạng cho cán bộ, công chức, viên chức và người lao động trong thời gian diễn ra Đại hội.

2. Chỉ đạo, quán triệt cán bộ, công chức, viên chức, người lao động thường xuyên thay đổi mật khẩu tài khoản thư điện tử công vụ; bảo đảm mật khẩu đủ mạnh theo quy định *(có ít nhất 08 ký tự, bao gồm chữ hoa, chữ thường, chữ số và ký tự đặc biệt)*; không lưu giữ mật khẩu trên trình duyệt Internet; tuyệt đối không sử dụng thư điện tử công vụ của tỉnh để đăng ký tài khoản trên các mạng xã hội, diễn đàn và các trang thông tin công cộng khác.

3. Thực hiện nghiêm túc Quyết định số 1744/QĐ-UBND ngày 03/12/2025 của Chủ tịch UBND tỉnh ban hành Phương án ứng cứu sự cố an toàn thông tin, an ninh mạng tỉnh Quảng Ngãi. Khi phát hiện dấu hiệu hoặc xảy ra sự cố mất an toàn thông tin, an ninh mạng, các cơ quan, đơn vị, địa phương kịp thời kích hoạt phương án ứng cứu, báo cáo sự cố về Công an tỉnh để hỗ trợ xử lý và tổng hợp, báo cáo UBND tỉnh, Bộ Công an theo quy định; không tự ý xử lý kéo dài, gây ảnh hưởng đến công tác bảo đảm an ninh, an toàn thông tin phục vụ Đại hội *(Phụ lục tình huống có thể phát sinh và phương án xử lý ban đầu gửi kèm theo)*.

4. Thành viên Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Quảng Ngãi *(theo Quyết định số 1573/QĐ-UBND ngày 14/11/2025 của Chủ tịch UBND tỉnh)* chủ động theo dõi, rà soát hệ thống mạng tại cơ quan, đơn vị quản lý; phối hợp xử lý sự cố, hỗ trợ công tác bảo đảm an toàn thông tin, an ninh mạng phục vụ Đại hội cho các cơ quan Đảng, Nhà nước trên địa bàn tỉnh khi có yêu cầu của Cơ quan thường trực Đội ứng cứu *(Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh)*.

5. Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh chủ trì, phối hợp với Trung tâm Chuyển đổi số và Đổi mới sáng tạo, Sở Khoa học và Công nghệ, Trung tâm Công báo Tin học - Văn phòng UBND tỉnh tăng cường công tác bảo đảm an toàn thông tin, an ninh mạng đối với các hệ thống thông tin dùng chung của tỉnh phục vụ Đại hội.

Các đơn vị quản trị, vận hành Trung tâm dữ liệu tỉnh và Trung tâm tích hợp dữ liệu Văn phòng UBND tỉnh có trách nhiệm bố trí cán bộ kỹ thuật trực, quản trị hệ thống 24/7; triển khai kế hoạch, phương án ứng phó, ứng cứu sự cố an toàn thông tin mạng; kịp thời phối hợp với Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao xử lý sự cố phát sinh trên địa bàn tỉnh.

6. Viettel Quảng Ngãi và VNPT Quảng Ngãi - đơn vị cung cấp dịch vụ giám sát an toàn, an ninh mạng tập trung (SOC) tỉnh Quảng Ngãi tiếp tục củng cố, ưu tiên nguồn lực cho nhiệm vụ giám sát, bảo vệ các hệ thống thông tin cấp độ 3 trên địa bàn tỉnh; triển khai giải pháp kỹ thuật rà quét, cảnh báo, phát hiện, xử lý mã độc; ưu tiên bảo đảm an toàn thông tin đối với các hệ thống trọng yếu phục vụ Đại hội gồm: Hệ thống quản lý và điều hành dùng chung trong các cơ quan nhà nước tỉnh Quảng Ngãi; Hệ thống thông tin giải quyết thủ tục hành chính tỉnh Quảng Ngãi; Cổng thông tin điện tử tỉnh Quảng Ngãi; Hệ thống thông tin báo cáo tỉnh Quảng Ngãi; Hệ thống quản lý công chức, viên chức và các hệ thống thông tin khác của tỉnh do đơn vị cung cấp dịch vụ công nghệ thông tin.

7. Trường hợp cần hỗ trợ xử lý, ứng cứu và khắc phục sự cố, đề nghị liên hệ các đầu mối kỹ thuật sau:

7.1. Trung tâm An ninh mạng quốc gia - Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an: Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT), điện thoại 0590.505.999, thư điện tử: vncert@nca.gov.vn.

7.2. Công an tỉnh Quảng Ngãi:

- Thượng tá Võ Văn Hoan - Phó Trưởng Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao; số điện thoại: 0980.331.268.

- Đại úy Phạm Nhật Trí - Cán bộ, Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao; số điện thoại: 0966.833.937.

- Thượng úy Hoàng Gia Bảo - Cán bộ, Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao; số điện thoại: 0964.634.357.

Đề nghị các cơ quan, đơn vị, địa phương quan tâm triển khai thực hiện./.

Nơi nhận:
- Như trên (t/hiện);
- Ủy ban nhân dân tỉnh (b/cáo);
- Cục An ninh mạng và phòng, chống TP sử dụng công nghệ cao, Bộ Công an (b/cáo);
- Lãnh đạo Công an tỉnh;
- Lưu: VT, ANM.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CÔNG AN TỈNH QUẢNG NGÃI

Đại tá Võ Văn Dương

PHỤ LỤC

Các tình huống có thể phát sinh và phương án xử lý ban đầu trong công tác bảo đảm an toàn thông tin, an ninh mạng phục vụ Đại hội Đại biểu toàn quốc lần thứ XIV của Đảng

(Kèm theo Công văn số 193/CAT-ANM ngày 12/01/2025 của Công an tỉnh)

1. Trang thông tin điện tử Đại hội bị tấn công từ chối dịch vụ (DdoS)

Cách nhận biết: Trang thông tin điện tử https://daihoidangtoanquoc.vn chậm bất thường hoặc không thể truy cập, thời gian tải trang tăng đột ngột, trình duyệt báo lỗi Gateway timeout, Service Unavailable (503)..; có một số dịch vụ trên web hoạt động, có dịch vụ thì không...

Hướng xử lý: Kịp thời trao đổi Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Công an tỉnh để phối hợp tiếp nhận, tổ chức xử lý. Đồng thời, triển khai các biện pháp kỹ thuật bảo đảm an ninh mạng, an toàn thông tin theo các quy định, hướng dẫn đã được ban hành, bảo đảm duy trì hoạt động ổn định, an toàn của Cổng thông tin điện tử phục vụ Đại hội *(theo Công văn số 2705/CAT-TM(ANM) ngày 09/10/2025 của Công an tỉnh).*

2. Cổng/Trang thông tin điện tử của các cơ quan Đảng, Nhà nước trên địa bàn tỉnh bị tấn công từ chối dịch vụ (DdoS)

Cách nhận biết: Cổng/Trang thông tin điện tử 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 sô dịch vụ trên web hoạt động, có dịch vụ thì không...

Hướng xử lý: Đội ứng cứu nội bộ xử lý sự cố phối hợp với 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.

3. Máy tính 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..

4. 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 daihoidangtq.ai, daihoidangxiv.com thay vì daihoidangtoanquoc.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, đại biểu 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.

5. 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 pay loads, 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.

6. Cổng/Trang 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.

7. 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 nhấp 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; thay đổi mật khẩu truy cập thiết bị mặc định do nhà sản xuất thiết lập (88888888, 11111111,...) hoặc các mật khẩu dễ đoán (12341234, 12345678,...); tắt quyền truy cập từ xa nếu thấy không cần thiết.