BỘ CÔNG AN
CÔNG AN TỈNH SƠN LA

Số: 194/CAT-ANM

V/v tăng cường bảo đảm an ninh, an toàn thông tin và ứng phó sự cố an ninh mạng phục vụ Đại hội đại biểu toàn quốc lần thứ XIV của Đảng

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

Sơn La, ngày 16 tháng 01 năm 2026

Kính gửi:
- Các Đảng ủy trực thuộc Tỉnh ủy;
- Các cơ quan tham mưu giúp việc Tỉnh ủy;
- Ủy ban Mặt trận Tổ quốc Việt Nam tỉnh;
- Các sở, ngành của Tỉnh;
- Các cơ quan Trung ương trên địa bàn tỉnh;
- UBND các xã, phường;
- Cơ quan báo chí, đài phát thanh, truyền hình, cơ quan thông tấn trên địa bàn tỉnh;
- Các doanh nghiệp viễn thông trên địa bàn tỉnh.

Đại hội Đại biểu toàn quốc lần thứ XIV của Đảng (*gọi tắt là Đại hội*) dự kiến tổ chức từ ngày 19/01/2026 đến ngày 25/01/2026 là sự kiện chính trị trọng đại của đất nước, thu hút sự quan tâm lớn ở trong nước và quốc tế. Việc bảo đảm an ninh, an toàn thông tin và sẵn sàng ứng phó sự cố an ninh mạng phục vụ Đại hội có ý nghĩa đặc biệt quan trọng, góp phần bảo đảm tổ chức Đại hội thành công, an toàn, tuyệt đối.

Thực hiện các chủ trương, chỉ đạo của Trung ương, Bộ Công an, Tỉnh ủy, Ủy ban nhân dân tỉnh về công tác bảo đảm an ninh, trật tự Đại hội đại biểu toàn quốc lần thứ XIV của Đảng; nhằm chủ động phòng ngừa, kịp thời phát hiện, ngăn chặn, xử lý các nguy cơ, sự cố mất an ninh, an toàn thông tin mạng, Công an tỉnh Sơn La đề nghị các cơ quan, đơn vị, địa phương, doanh nghiệp có liên quan tổ chức triển khai thực hiện nghiêm túc các nội dung sau:

1. Quán triệt, triển khai có hiệu quả các tình huống bảo đảm 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 tình huống kèm theo)*.

2. Các đơn vị chủ quản tăng cường công tác bảo đảm an ninh, an toàn thông tin đối với trang thiết bị phục vụ đưa tin về Đại hội bao gồm: Hệ thống mạng LAN, 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...; phối hợp với đơn vị cung cấp dịch vụ, bố trí lực lượng thường trực giám sát 24/7 để kịp thời phát hiện, ngăn chặn, ứng phó, khắc phục sự

cố an toàn thông tin, an ninh mạng, bảo đảm các hệ thống hoạt động ổn định, thông suốt, không bị gián đoạn.

3. Tăng cường 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. Khi phát hiện sự cố an ninh mạng hoặc dấu hiệu mất an ninh, an toàn thông tin, các đơn vị kịp thời trao đổi về Công an tỉnh *(qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, SĐT: 069.2680.415)* để điều phối Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Sơn La tham gia phối hợp, xử lý theo quy định./.

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

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Đại tá Trần Thanh Sơn

MỘT SỐ TÌNH HUỐNG CỤ THỂ VÀ HƯỚNG XỬ LÝ BAN ĐẦU

(Kèm theo Công văn số 194/CAT-ANM ngày 16/01/2026 của Công an tỉnh Sơn La)

1. Trang thông tin điện tử đưa tin tuyên truyền về Đại hội bị tấn công từ chối dịch vụ DDoS

- Cách nhận biết: Trang thông tin điện tử https://dangcongsan.org.vn/sonla 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: Đội ứng cứu 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.

2. 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, ransomware.

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 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.

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./.