

Số: 4832/ CAT-PA05

Gia Lai, ngày 22 tháng 12 năm 2025

V/v tăng cường công tác bảo đảm an toàn thông tin, an ninh mạng phục vụ bầu cử ĐBQH khóa XVI và đại biểu HĐND các cấp nhiệm kỳ 2026-2031

Kính gửi:

- Các sở, ban, ngành, đoàn thể trên địa bàn tỉnh;
- Ủy ban nhân dân cấp xã;
- Các doanh nghiệp cung cấp dịch vụ viễn thông, Internet.

Thực hiện ý kiến chỉ đạo của đồng chí Bí thư Tỉnh ủy về công tác bảo đảm an toàn thông tin, an ninh mạng phục vụ cuộc bầu cử đại biểu Quốc hội khóa XVI và đại biểu Hội đồng nhân dân các cấp nhiệm kỳ 2026-2031; Công an tỉnh (cơ quan chuyên trách về an toàn thông tin mạng của UBND tỉnh) đề nghị các đơn vị, địa phương, chủ quản hệ thống thông tin, đơn vị quản lý Công thông tin điện tử khẩn trương triển khai các biện pháp sau:

### **I. XÁC ĐỊNH CẤP ĐỘ VÀ CƯỜNG CỐ HẠ TẦNG MẠNG**

1. Hoàn thiện hồ sơ đề xuất cấp độ an toàn hệ thống thông tin:

Các đơn vị rà soát, xây dựng và hoàn thiện hồ sơ đề xuất cấp độ an toàn hệ thống thông tin cho các hệ thống thuộc phạm vi quản lý. Nhiệm vụ này có vai trò trọng tâm trong việc thiết lập cơ sở pháp lý và kỹ thuật để xác định và triển khai các phương án bảo đảm an toàn thông tin, an ninh mạng phù hợp và tuân thủ quy định hiện hành.

2. Quy hoạch phân vùng mạng:

Thực hiện khảo sát, đánh giá hiện trạng và thiết kế mô hình mạng phân chia thành các vùng riêng biệt (tách biệt logic hoặc vật lý), bao gồm: Vùng mạng trung lập, Vùng mạng ứng dụng, Vùng mạng cơ sở dữ liệu, Vùng mạng quản trị...

3. Kiểm soát truy cập:

Việc truy cập giữa các vùng mạng cần được thực hiện thông qua thiết bị tường lửa (Firewall) có khả năng tích hợp tính năng phát hiện và phòng, chống xâm nhập (IPS/IDS) cũng như phòng, chống mã độc ở lớp mạng.

4. Triển khai các phương án kỹ thuật đồng bộ:

- Quản lý truy cập và quản trị hệ thống từ xa an toàn;
- Cân bằng tải, dự phòng nóng cho thiết bị mạng chính;
- Phòng, chống tấn công từ chối dịch vụ (DDoS);
- Tường lửa ứng dụng web (WAF);
- Giám sát an toàn thông tin tập trung;
- Sao lưu dự phòng tập trung;
- Quản lý tập trung phần mềm phòng, chống mã độc;

- Bảo mật hệ thống thư điện tử;
- Phòng, chống thất thoát dữ liệu;
- Dự phòng kết nối Internet cho máy chủ dịch vụ.

## **II. QUẢN LÝ VẬN HÀNH VÀ CHÍNH SÁCH NGƯỜI DÙNG**

### **1. Cập nhật bản vá và rà quét lỗ hổng:**

Chủ động cập nhật đầy đủ các bản vá bảo mật cho hệ điều hành và ứng dụng; đồng thời cài đặt phần mềm phòng, chống mã độc có bản quyền trên toàn bộ máy chủ và máy tính người dùng. Thực hiện rà quét lỗ hổng bảo mật và mã độc định kỳ trên các hệ thống, bao gồm Công thông tin, Thư điện tử, Quản lý văn bản và các nền tảng tương tự.

### **2. Tăng cường quản lý tài khoản:**

Thực hiện phân cấp và phân quyền tài khoản dựa trên chức năng, nhiệm vụ cụ thể (tuân thủ nguyên tắc quyền tối thiểu); đồng thời, lưu trữ nhật ký sử dụng. Thiết lập các giao thức mạng có khả năng mã hóa mạnh mẽ cho mục đích quản trị từ xa; đồng thời, giới hạn địa chỉ IP quản trị trong phạm vi hệ thống.

## **III. GIÁM SÁT VÀ ỨNG CỨU SỰ CỐ**

1. Triển khai các biện pháp giám sát liên tục (24/7) nhằm bảo đảm khả năng ứng phó kịp thời với các sự cố:

- Giám sát tình trạng hoạt động thiết bị;
- Giám sát phát hiện tấn công DoS/DDoS;
- Giám sát kết nối bất thường, mã độc trong mạng;
- Giám sát hành vi rà quét dịch vụ từ bên trong;
- Giám sát tấn công khai thác lỗ hổng đối với thiết bị công khai trên Internet.

2. Thiết lập kênh liên lạc thường xuyên và phối hợp chặt chẽ với Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh: Sẵn sàng tham gia mạng lưới ứng cứu sự cố quốc gia; chia sẻ thông tin, thống nhất phương án xử lý khi phát hiện các cuộc tấn công mạng quy mô lớn hoặc phức tạp. Khi phát hiện sự cố mất an toàn thông tin hoặc có dấu hiệu bị tấn công mạng, các đơn vị phải:

- Thực hiện quy trình báo cáo sự cố theo đúng quy định của pháp luật (Báo cáo ban đầu, báo cáo diễn biến, báo cáo kết thúc) gửi về Công an tỉnh (qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao);
- Thực hiện các biện pháp sơ bộ để xác minh, ngăn chặn sự cố lan rộng (như ngắt kết nối mạng, cô lập máy chủ bị nhiễm) và ghi nhận lại hiện trạng;
- Tuyệt đối không che giấu sự cố dẫn đến hậu quả nghiêm trọng.

## **IV. CÔNG TÁC TUYÊN TRUYỀN**

Các cơ quan, đơn vị, địa phương chủ động phối hợp với các tổ chức đoàn thể tổ chức quán triệt, tuyên truyền, phổ biến sâu rộng tới toàn thể cán bộ, đảng viên, công chức, viên chức và quần chúng nhân dân các nội dung sau:

1. Tập trung nâng cao nhận thức, trách nhiệm của từng cá nhân về vai trò, tầm quan trọng của công tác bảo đảm an toàn thông tin, an ninh mạng trong tình hình mới; coi đây là nhiệm vụ thường xuyên, liên tục và cấp bách.

2. Nêu cao tinh thần cảnh giác, chủ động nhận diện, phân tích và đấu tranh, phản bác các quan điểm sai trái, thù địch, thông tin sai lệch, xấu độc. Đồng thời, tích cực "phủ xanh" không gian mạng bằng cách đẩy mạnh chia sẻ, lan tỏa các thông tin chính thống, chính xác, có giá trị tích cực từ các nguồn tin cậy của Đảng và Nhà nước.

3. Thường xuyên hướng dẫn, trang bị kỹ năng an toàn thông tin cơ bản cho người dùng cuối. Trong đó, yêu cầu cán bộ, người dân tuyệt đối không tự ý chia sẻ, phát tán các thông tin, tài liệu chưa được kiểm chứng hoặc có nội dung độc hại; không truy cập (click) vào các đường dẫn liên kết lạ, không rõ nguồn gốc được gửi qua mạng xã hội, thư điện tử hoặc tin nhắn SMS để tránh nguy cơ bị chiếm quyền kiểm soát thiết bị hoặc đánh cắp dữ liệu.

Đề nghị Thủ trưởng các đơn vị, địa phương nghiêm túc thực hiện. Trong quá trình triển khai, phát sinh khó khăn, vướng mắc trao đổi về Công an tỉnh (*qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao; đầu mối liên hệ: Thiếu tá Nguyễn Tuấn Anh, Cán bộ, SĐT: 0977.352.785, Email: ant-pa05@cat.gialai.gov.vn; Thiếu tá Ung Quốc Cường, Cán bộ, SĐT: 0987.174.292 Email: ttanm@cat.gialai.gov.vn*) để tổng hợp và báo cáo theo quy định. *ctb*

**Nơi nhận:**

- Như trên;
- Cục A05 (để báo cáo);
- Chủ tịch UBND tỉnh (để báo cáo);
- Văn phòng UBND tỉnh (để theo dõi)
- Giám đốc Công an tỉnh (để báo cáo);
- Phòng PV01 (để theo dõi);
- Lưu: Văn thư (CAT), PA05 (Đ2).



**Đại tá Nguyễn Chí Linh**