

Số: /KH-TBATANM

An Giang, ngày tháng năm 2025

KẾ HOẠCH
Kiểm tra, giám sát an ninh, an toàn
các hệ thống thông tin trên địa bàn tỉnh

Thực hiện Công văn số 102/UBND-KGVX ngày 15/7/2025 UBND tỉnh về việc triển khai các giải pháp đáp ứng yêu cầu sắp xếp đơn vị hành chính theo mô hình mới; Công văn 104/UBND-KGVX ngày 15/7/2025 của UBND tỉnh về việc khẩn trương khắc phục các tồn tại, hạn chế phục vụ triển khai thực hiện các nhiệm vụ đảm bảo mô hình chính quyền mới sẵn sàng hoạt động thông suốt phục vụ người dân và doanh nghiệp. Tiểu ban An toàn, an ninh mạng tỉnh xây dựng kế hoạch kiểm tra cụ thể như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Kiểm tra thực trạng an ninh mạng, an toàn thông tin đối với hệ thống thông tin trên địa bàn tỉnh, kịp thời phát hiện các điểm yếu, lỗ hổng bảo mật, các vấn đề tồn tại của các hệ thống thông tin dễ dẫn đến nguy cơ mất an ninh mạng, an toàn thông tin, từ đó đề ra những giải pháp khắc phục kịp thời nhằm đảm bảo an ninh mạng, an toàn thông tin đối với hệ thống thông tin trên địa bàn tỉnh; rà soát, kiểm tra đề xuất phê duyệt cấp độ, vận hành và phương án đảm bảo an ninh mạng, an toàn thông tin từ đó phát hiện các điểm yếu, lỗ hổng bảo mật, nguy cơ mất an ninh mạng, an toàn thông tin; kiểm tra, đảm bảo tuyệt đối an ninh, an toàn đối với các hệ thống tại Trung tâm Phục vụ hành chính công các cấp, qua đó kiến nghị, đề xuất nâng cấp, thay thế mới các thiết bị cũ, công suất thấp, có nguy cơ bị tấn công mạng.

2. Quyết liệt trong chỉ đạo, bảo đảm phân công trách nhiệm rõ ràng, chặt chẽ, nêu cao tinh thần trách nhiệm của người đứng đầu các đơn vị, sâu sát trong việc hoàn thành các hạng mục công việc được phân công.

3. Quá trình kiểm tra phải đảm bảo tuyệt đối an ninh, an toàn hệ thống và dữ liệu; bảo vệ bí mật nhà nước và bảo vệ dữ liệu cá nhân theo đúng quy định của pháp luật.

II. NỘI DUNG THỰC HIỆN

- Kiểm tra, khắc phục các lỗ hổng, các vấn đề tồn tại của các hệ thống như: Phần mềm chưa kích hoạt bản quyền; Phần mềm bẻ khóa bản quyền có chứa mã độc; Windows Firewall tại các máy trạm bị dẫn đến nguy cơ lây lan mã độc; Lưu mật khẩu trên trình duyệt; Máy tính phục vụ công dân, doanh nghiệp

lưu lại tài liệu của người dân, doanh nghiệp; Cấp quyền “Administrator” cho khách dẫn tới nguy cơ cài đặt phần mềm độc hại hoặc đánh cắp dữ liệu cá nhân, doanh nghiệp; Thiết bị Kiosk lấy số chưa được cài đặt phần mềm diệt virus chuyên dụng; Chưa bố trí nhân sự đảm bảo an toàn thông tin hệ thống...

- Kiểm tra việc đề xuất phê duyệt cấp độ đối với hệ thống thông tin của các sở, ngành, UBND các xã, phường, đặc khu; việc vận hành và phương án đảm bảo an ninh mạng, an toàn thông tin theo hồ sơ đề xuất cấp độ đã được phê duyệt, từ đó phát hiện các điểm yếu, lỗ hổng bảo mật, nguy cơ mất an ninh mạng, an toàn thông tin để kịp thời có biện pháp khắc phục ngay.

- Kiểm tra vấn đề an ninh, an toàn đối với các hệ thống tại các Trung tâm Phục vụ hành chính công các cấp, phát hiện, khắc phục các lỗ hổng, các vấn đề tồn tại của các hệ thống; Kiểm tra, đánh giá các thiết bị, máy tính, phần mềm được trang bị tại các Trung tâm Phục vụ hành chính công các cấp, nếu đã cũ hoặc công suất thấp, có nguy cơ bị tấn công mạng... thì có kiến nghị đối với đơn vị để tính toán đề xuất trang cấp mới, đảm bảo phục vụ công tác.

III. ĐỐI TƯỢNG, THỜI GIAN, THÀNH PHẦN KIỂM TRA

1. Đối tượng kiểm tra: kiểm tra trực tiếp các sở, ban, ngành trên địa bàn tỉnh; UBND các xã, phường, đặc khu; Trung tâm Phục vụ hành chính công của tỉnh và của các xã, phường, đặc khu (có danh sách cụ thể kèm theo).

2. Thời gian kiểm tra: bắt đầu từ tháng 9/2025 cho đến khi kết thúc kiểm tra tất cả sở, ngành và các xã, phường, đặc khu (có lịch thông báo cụ thể sau).

3. Thành phần

a) Thành phần Đoàn kiểm tra:

- Lãnh đạo Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao Công an tỉnh - Trưởng đoàn;

- Lãnh đạo Phòng Chuyển đổi số - Sở Khoa học và Công nghệ - Phó trưởng đoàn;

- Các thành viên:

+ Chuyên viên Văn phòng Ủy ban nhân dân tỉnh;

+ Cán bộ Phòng Chuyển đổi số - Sở Khoa học và Công nghệ;

+ Cán bộ Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao Công an tỉnh;

+ Cán bộ Phòng Cảnh sát quản lý hành chính về trật tự xã hội Công an tỉnh.

+ Cán bộ Phòng Kỹ thuật nghiệp vụ và Ngoại tuyến Công an tỉnh.

(có ban hành Quyết định riêng).

b) Thành phần làm việc với Đoàn kiểm tra

- Đối với các cơ quan, đơn vị, sở, ngành: đại diện Lãnh đạo cơ quan; đại diện các phòng có liên quan; Cán bộ quản trị hệ thống mạng.

- Đối với địa phương: Đại diện Lãnh đạo UBND xã, phường, đặc khu; Đại diện Văn phòng UBND xã, phường, đặc khu; Đại diện các phòng có liên quan; Cán bộ quản trị hệ thống mạng.

IV. PHƯƠNG PHÁP KIỂM TRA

- Khi nhận được thông báo kiểm tra, các đơn vị, địa phương được kiểm tra chuẩn bị báo cáo bằng văn bản (*nội dung: tình hình, kết quả công tác bảo đảm an ninh, an toàn hệ thống thông tin cấp tỉnh và cấp xã; hạ tầng CNTT các máy tính, thiết bị của hệ thống đặt tại các Trung tâm Phục vụ hành chính công các cấp; việc đề xuất phê duyệt cấp độ, vận hành và phương án đảm bảo an ninh mạng, an toàn thông tin đối với hệ thống thông tin của đơn vị*) gửi về Tiểu ban An toàn, An ninh mạng tỉnh (qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) **trước ngày 25/9/2025** để chuẩn bị phục vụ công tác kiểm tra.

- Khi Đoàn đến làm việc trực tiếp, đơn vị được kiểm tra trình bày báo cáo, sau đó Đoàn kiểm tra có thể yêu cầu giải trình những nội dung cần làm rõ. Tiếp theo, Đoàn kiểm tra nêu nội dung, yêu cầu cần chuẩn bị để phục vụ công tác kiểm tra thực tế.

- Các thành viên theo chức năng, nhiệm vụ được giao tiến hành kiểm tra trực tiếp trên các hệ thống thông tin tại cơ quan, đơn vị, địa phương được kiểm tra; các máy tính, thiết bị có liên quan đến các dịch vụ công, hệ thống thông tin của Trung tâm Phục vụ hành chính công các cấp trên địa bàn tỉnh.

- Sau khi kiểm tra trực tiếp, các thành viên Đoàn kiểm tra tổng hợp, thảo luận, thống nhất nội dung biên bản, ghi nhận kết quả kiểm tra, kiến nghị chấn chỉnh, khắc phục hạn chế, xử lý vi phạm (*nếu có*).

- Công bố biên bản ghi nhận kết quả kiểm tra; Đoàn kiểm tra hướng dẫn đơn vị được kiểm tra khắc phục những tồn tại, hạn chế trong quá trình thực hiện công tác bảo đảm an ninh, an toàn hệ thống thông tin của các đơn vị, địa phương và các Trung tâm Phục vụ hành chính công các cấp.

- Sau kiểm tra, Đoàn kiểm tra tổng hợp, báo cáo kết quả kiểm tra với Tiểu ban An toàn, An ninh mạng tỉnh nắm, chỉ đạo.

V. TỔ CHỨC THỰC HIỆN

1. Giao Bộ phận Thường trực Tổ An ninh mạng Công an tỉnh - Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao tham mưu Tiểu ban ban hành Quyết định thành lập đoàn kiểm tra, Lịch kiểm tra, tập hợp kết quả kiểm tra của từng cơ quan, đơn vị, địa phương tham mưu Tiểu ban báo cáo UBND tỉnh theo quy định. Đề xuất, kiến nghị chấn chỉnh, khắc phục hạn chế, xử lý trách nhiệm đối với các trường hợp vi phạm (nếu có).

2. Công an tỉnh (Phòng Hậu cần) bố trí phương tiện phục vụ Đoàn kiểm tra theo kế hoạch.

3. Quá trình thực hiện có khó khăn, vướng mắc hoặc thay đổi về thời gian, thành phần so với kế hoạch kiểm tra, các cơ quan, đơn vị, địa phương chủ động báo cáo Đoàn kiểm tra (qua Bộ phận thường trực Tổ An ninh mạng Công an tỉnh - Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao; đầu mối liên hệ: **Thiếu tá Trần Thanh Trường - Phó Đội trưởng, Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao - Số điện thoại: 0899.522799**) trước 03 ngày để tập hợp, báo cáo Trưởng Đoàn kiểm tra xem xét, điều chỉnh cho phù hợp./.

Nơi nhận:

- CT UBND tỉnh;
- PCT Nguyễn Thanh Phong;
- Đ/c Giám đốc CAT (để p/h chỉ đạo);
- Công an tỉnh (PA05);
- CVP, PCVP Thái Thị Duy Quyên;
- Các đơn vị thành viên Đoàn kiểm tra;
- Các sở, ban, ngành được kiểm tra;
- UBND các xã, phường, đặc khu;
- TT CBTH;
- Phòng KGVX;
- Lưu: VT, ntgiang.

TRƯỞNG TIỂU BAN

CHỦ TỊCH UBND TỈNH
Hồ Văn Mừng