ỦY BAN NHÂN DÂN TỈNH TUYÊN QUANG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 245 /UBND-KH&CĐS V/v tăng cường đảm bảo an toàn thông tin mạng sau sáp nhập tỉnh	*Tuyên Quang, ngày 15 tháng 7 năm 2025*

Kính gửi:
- Các sở, ban, ngành thuộc tỉnh;
- Văn phòng Ủy ban nhân dân tỉnh;
- Chủ tịch Ủy ban nhân dân các xã, phường.
- Các doanh nghiệp cung cấp dịch vụ viễn thông, Internet.

Căn cứ Kế hoạch số 02-KH/BCĐTW ngày 19 tháng 6 năm 2025 của Ban Chỉ đạo Trung ương về việc thúc đẩy chuyển đổi số liên thông, đồng bộ, nhanh, hiệu quả đáp ứng yêu cầu sắp xếp tổ chức bộ máy của hệ thống chính trị;

Căn cứ Kế hoạch số 396/KH-BCA-C06 ngày 28 tháng 6 năm 2025 của Bộ Công an về việc thực hiện cao điểm đảm bảo an ninh mạng, an toàn thông tin trong giai đoạn chuyển sang mô hình chính quyền địa phương 02 cấp;

Thực hiện chỉ đạo của Chính phủ, Bộ Công an về đảm bảo tuyệt đối an ninh, an toàn cho hệ thống dịch vụ công và hệ thống điều hành của các bộ, ngành, địa phương vận hành thông suốt không gián đoạn sau sáp nhập, sắp xếp tổ chức bộ máy chính quyền địa phương 02 cấp. Để nâng cao tính chủ động, khắc phục kịp thời sơ hở, hạn chế và phát huy vai trò, trách nhiệm của người đứng đầu cơ quan, đơn vị, địa phương trong công tác lãnh đạo, chỉ đạo đảm bảo an toàn, an ninh mạng hệ thống thông tin trọng yếu,

Chủ tịch Ủy ban nhân dân tỉnh chỉ đạo:

1. Thủ trưởng các sở, ban, ngành tỉnh; Chủ tịch Ủy ban nhân dân các xã, phường thực hiện quyết liệt, có hiệu quả các nội dung sau:

- Chỉ đạo rà soát hệ thống thông tin thuộc phạm vi quản lý, duy trì vận hành cơ chế giám sát an toàn, an ninh mạng hệ thống hiện hành và bảo vệ dữ liệu hệ thống cũ phục vụ sử dụng, khai thác sau hợp nhất ***(hoàn thành trước ngày 19/7/2025)***. Xác định rõ trách nhiệm của người đứng đầu cơ quan, đơn vị, địa phương trong công tác đảm bảo an ninh, an toàn hệ thống thông tin thuộc phạm vi phụ trách.

- Trực tiếp chỉ đạo và phụ trách công tác bảo đảm an toàn thông tin mạng; chịu trách nhiệm trước pháp luật và Chủ tịch Ủy ban nhân dân tỉnh nếu để hệ thống thông tin thuộc phạm vi quản lý không bảo đảm an toàn thông tin mạng, để xảy ra sự cố nghiêm trọng; thường xuyên quán triệt cán bộ, công chức, viên chức tuân thủ, chấp hành nghiêm quy định, quy chế quản lý, bảo mật, khai thác, vận hành các hệ thống thông tin, quản trị người dùng và bảo vệ bí mật nhà nước trên không gian mạng.

- Điều chỉnh, bổ sung hoặc ban hành mới quy chế đảm bảo an ninh an toàn hệ thống thông tin; rà soát, cập nhật, hoàn thiện, ban hành Phương án đảm bảo an toàn thông tin theo cấp độ hoặc trình cấp có thẩm quyền phê duyệt; xây dựng quy trình quản lý, vận hành các hệ thống thông tin, thiết bị đầu cuối thuộc phạm vi quản lý phục vụ vận hành thông suốt chính quyền hai cấp ***(hoàn thành trước ngày 29/7/2025)***.

2. Công an tỉnh (Cơ quan chuyên trách về đảm bảo an toàn thông tin mạng trên địa bàn tỉnh)

- Chỉ đạo triển khai đồng bộ, quyết liệt các giải pháp, nhiệm vụ về đảm bảo an toàn thông tin mạng, phối hợp chặt chẽ với các cơ quan chủ quản, đơn vị vận hành hệ thống thông tin trên địa bàn tỉnh nắm bắt lộ trình tích hợp các hệ thống thông tin sau sáp nhập để điều chỉnh quy mô, phạm vi giám sát an ninh mạng của hệ thống SOC, bảo đảm nguyên tắc các hệ thống thông tin quan trọng phải được giám sát an ninh mạng, bao gồm cả hệ thống cũ còn tiếp tục sử dụng, khai thác hồ sơ, dữ liệu sau hợp nhất.

- Phối hợp với Văn phòng Ủy ban nhân dân tỉnh, Sở Khoa học và Công nghệ rà soát, xác định chính xác tài khoản người dùng tại các đơn vị, địa phương có kết nối Cổng dịch vụ công một cửa; rà soát thiết bị đầu cuối phục vụ giải quyết thủ tục hành chính để triển khai, bổ sung giải pháp phòng chống mã độc tập trung.

- Yêu cầu các doanh nghiệp cung cấp dịch vụ viễn thông, Internet, an toàn thông tin mạng cho các hệ thống thông tin của đơn vị, địa phương được giao quản lý, vận hành thực hiện kết nối, chia sẻ dữ liệu giám sát về Trung tâm an ninh mạng quốc gia *(qua đầu mối tiếp nhận là Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao Công an tỉnh; email: phonganm.congantinh@tuyenquang.gov.vn)* để hỗ trợ giám sát, điều phối ứng phó sự cố. Duy trì giám sát 24/24h đối với toàn bộ các hệ thống thông tin và cập nhật dữ liệu cảnh báo SOC, dữ liệu cảnh báo của Hệ thống phòng chống mã độc tập chung, dữ liệu cảnh báo an ninh mạng theo chỉ đạo, hướng dẫn của Trung tâm an ninh mạng quốc gia ***(hoàn thành trong tháng 7/2025).***

- Kiện toàn Tổ An ninh, an toàn thông tin Công an tỉnh Tuyên Quang, định kỳ (đột xuất) kiểm tra, đánh giá an toàn thông tin ninh mạng các hệ thống thông tin sau hợp nhất, trọng tâm là các thiết bị đầu cuối, tài khoản quản trị, tài khoản người dùng tại Trung tâm Phục vụ hành chính công cấp tỉnh, xã và kiến nghị xử lý nghiêm vi phạm

3. Văn phòng Ủy ban nhân dân tỉnh

Chỉ đạo Trung tâm Phục vụ hành chính công tỉnh khắc phục triệt để sơ hở, tồn tại, hạn chế về bảo đảm an ninh, an toàn hệ thống thông tin qua kiểm tra, đánh giá; quản lý chặt chẽ, áp dụng đầy đủ các biện pháp bảo mật ngăn ngừa nguy cơ lộ, mất, bị chiếm quyền tài khoản người dùng ***(hoàn thành trước 19/7/2025)***.

4. Sở Khoa học và Công nghệ

- Phối hợp với doanh nghiệp cung cấp dịch vụ viễn thông, Internet, an toàn thông tin mạng, công nghệ thông tin tại địa phương thành lập Tổ thường trực, bố trí lực lượng giám sát 24/7 cho các hệ thống dịch vụ công, hệ thống thông tin phục vụ chỉ đạo, điều hành theo cam kết, hợp đồng đã ký kết, kịp thời phát hiện, ứng phó các sự cố an ninh mạng, an toàn thông tin, bảo đảm các hệ thống phục vụ mô hình chính quyền địa phương 02 cấp hoạt động ổn định, thông suốt không bị gián đoạn ***(hoàn thành trước 19/7/2025).***

- Chỉ đạo đơn vị hợp đồng cung cấp dịch vụ vận hành Cổng dịch vụ công triển khai đầy đủ giải pháp đảm bảo an toàn thông tin mạng cấp độ 3; đồng thời quản lý chặt chẽ API kết nối Cổng dịch vụ công tỉnh với Cơ sở dữ liệu quốc gia về dân cư, tuân thủ đúng quy định về bảo mật an toàn thông tin.

5. Chủ tịch Ủy ban nhân dân các xã, phường

Chỉ đạo Trung tâm Phục vụ hành chính công bám sát hướng dẫn, yêu cầu của cơ quan chuyên trách chủ động kiểm tra, chấn chỉnh, khắc phục ngay sơ hở, tồn tại hạn chế và triển khai đồng bộ các giải pháp đảm bảo an ninh, an toàn hệ thống thông tin thuộc phạm vi phụ trách; duy trì thường xuyên cơ chế phối hợp, trao đổi thông tin, xử lý kịp thời những vấn đề phát sinh, đảm bảo an toàn hệ thống, thiết bị đầu cuối, tài khoản người dùng.

6. Các Doanh nghiệp cung cấp dịch vụ viễn thông, Internet

Nghiên cứu, triển khai các giải pháp trên thiết bị truy cập mạng Internet do doanh nghiệp cung cấp cho người sử dụng để bảo vệ người sử dụng không truy cập vào các nguồn thông tin vi phạm pháp luật và ngăn chặn nguy cơ mất an toàn thông tin mạng; thực hiện kết nối, chia sẻ thông tin, dữ liệu theo hướng dẫn của Bộ Khoa học và Công nghệ.

Căn cứ ý kiến chỉ đạo, các cơ quan, đơn vị, địa phương nghiêm túc triển khai, thực hiện. Báo cáo kết quả triển khai thực hiện về Công an tỉnh (qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao; điện thoại: 0988507990; Email: phonganm.congantinh@tuyenquang.gov.vn) **trước ngày 30/7/2025** để tổng hợp, báo cáo theo quy định./.

Nơi nhận:
- Như trên;
- Thường trực Tỉnh ủy (b/c);
- Thường trực HĐND tỉnh (b/c);
- Chủ tịch UBND tỉnh;
- Các Phó Chủ tịch UBND tỉnh;
- Lãnh dạo VP UBND tỉnh;
- Trung tâm Thông tin Công báo;
- Trung tâm Phục vụ HCC;
- Lưu: VT, KH&CĐS.

CHỦ TỊCH

ỦY BAN NHÂN DÂN TỈNH TUYÊN QUANG

Phan Huy Ngọc