

**ỦY BAN NHÂN DÂN
TỈNH HƯNG YÊN**

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

Số: 4626/UBND-NC
V/v bảo đảm an ninh mạng,
an ninh thông tin, an ninh dữ liệu

Hưng Yên, ngày 17 tháng 7 năm 2026

Kính gửi:

- Ủy ban Mặt trận Tổ quốc Việt Nam tỉnh và các tổ chức chính trị - xã hội tỉnh;
- Các Ban, cơ quan thuộc Tỉnh ủy;
- Các Ban của Hội đồng nhân dân tỉnh;
- Các sở, ban, ngành tỉnh;
- Ủy ban nhân dân các xã, phường.

Thời gian qua, tình hình an ninh mạng, an ninh thông tin và an ninh dữ liệu tiếp tục diễn biến phức tạp; các cuộc tấn công mạng nhằm vào cơ quan nhà nước, tổ chức, doanh nghiệp có xu hướng gia tăng cả về quy mô, mức độ và phương thức, thủ đoạn. Nhiều vụ việc làm lộ, lọt dữ liệu, mã hóa dữ liệu, chiếm quyền điều khiển hệ thống thông tin đã gây ảnh hưởng đến hoạt động của cơ quan, tổ chức và tiềm ẩn nguy cơ đe dọa an ninh quốc gia, trật tự, an toàn xã hội.

Mặc dù trên địa bàn tỉnh chưa phát hiện vụ việc đặc biệt nghiêm trọng liên quan đến an ninh mạng, an ninh thông tin và an ninh dữ liệu, song qua công tác nắm tình hình, đã phát hiện một số thiết bị, hệ thống thông tin bị lây nhiễm mã độc, tiềm ẩn nguy cơ bị tấn công, xâm nhập trái phép nếu không được kịp thời phát hiện, xử lý và triển khai đầy đủ các biện pháp bảo đảm an ninh mạng theo quy định.

Để chủ động phòng ngừa, nâng cao hiệu lực, hiệu quả công tác bảo đảm an ninh mạng, an ninh thông tin và an ninh dữ liệu trên địa bàn tỉnh; thực hiện Công văn số 2656/BCA-A05 ngày 02/6/2026 của Bộ Công an về việc hướng dẫn triển khai công tác bảo đảm an ninh mạng, an ninh thông tin, an ninh dữ liệu, Ủy ban nhân dân tỉnh có ý kiến như sau:

1. Các sở, ban, ngành tỉnh, UBND các xã, phường:

- Tổ chức quán triệt, triển khai thực hiện nghiêm các quy định của pháp luật về an ninh mạng, an toàn thông tin, bảo vệ dữ liệu, bảo vệ bí mật nhà nước và các văn bản hướng dẫn của Bộ Công an; chủ động nghiên cứu, áp dụng Tiêu chuẩn quốc gia TCVN 14423:2025 "An ninh mạng - Yêu cầu đối với hệ thống thông tin quan trọng" và các nội dung hướng dẫn tại Phụ lục kèm theo Công văn này phù hợp với điều kiện thực tế của cơ quan, đơn vị.

- Rà soát, đánh giá toàn diện công tác bảo đảm an ninh mạng, an ninh thông tin và an ninh dữ liệu đối với các hệ thống thông tin thuộc phạm vi quản lý; kịp thời khắc phục các tồn tại, hạn chế, lỗ hổng, điểm yếu về bảo mật; rà soát, bổ sung, hoàn thiện các quy chế, quy trình quản lý, vận hành, bảo đảm an ninh mạng theo quy định.

- Tăng cường công tác quản lý rủi ro, giám sát an ninh mạng; triển khai đầy đủ các biện pháp phòng ngừa, phát hiện, ngăn chặn, ứng phó và khắc phục sự cố

an ninh mạng; chủ động bảo vệ dữ liệu, bảo vệ bí mật nhà nước và dữ liệu cá nhân trong quá trình quản lý, khai thác, sử dụng hệ thống thông tin.

- Người đứng đầu các cơ quan, đơn vị, địa phương chịu trách nhiệm trước Chủ tịch UBND tỉnh về công tác bảo đảm an ninh mạng, an ninh thông tin và an ninh dữ liệu đối với các hệ thống thông tin thuộc phạm vi quản lý; bố trí nguồn lực phù hợp, thường xuyên kiểm tra, đôn đốc việc tổ chức thực hiện, không để xảy ra lộ, lọt bí mật nhà nước, dữ liệu cá nhân hoặc sự cố an ninh mạng nghiêm trọng do nguyên nhân chủ quan.

- Định kỳ hoặc khi có yêu cầu, tổ chức tự kiểm tra, đánh giá việc thực hiện các quy định về bảo đảm an ninh mạng, an ninh thông tin và an ninh dữ liệu; kịp thời khắc phục các tồn tại, hạn chế và phối hợp với Công an tỉnh trong công tác kiểm tra, hướng dẫn, xử lý các sự cố an ninh mạng theo quy định.

2. Giao Công an tỉnh chủ trì, phối hợp với các cơ quan, đơn vị, địa phương liên quan theo dõi, nắm tình hình, tăng cường rà soát, phát hiện, cảnh báo kịp thời các nguy cơ, lỗ hổng, điểm yếu về an ninh mạng đối với các hệ thống thông tin; hướng dẫn, hỗ trợ các cơ quan, đơn vị triển khai các biện pháp bảo đảm an ninh mạng, xử lý, bóc gỡ mã độc, ứng phó, khắc phục sự cố tấn công mạng; tổng hợp tình hình, kịp thời tham mưu UBND tỉnh chỉ đạo xử lý các vấn đề phát sinh theo thẩm quyền.

3. Đề nghị các Ban, cơ quan thuộc Tỉnh ủy; các Ban của Hội đồng nhân dân tỉnh; Ủy ban Mặt trận Tổ quốc Việt Nam tỉnh và các tổ chức chính trị - xã hội tỉnh căn cứ chức năng, nhiệm vụ được giao, phối hợp triển khai thực hiện các nội dung của Công văn này và Phụ lục kèm theo đối với các hệ thống thông tin thuộc phạm vi quản lý; tăng cường công tác bảo đảm an ninh mạng, an ninh thông tin và an ninh dữ liệu, bảo đảm đồng bộ, hiệu quả theo quy định.

Yêu cầu các sở, ban, ngành, Ủy ban nhân dân các xã, phường; đề nghị các Ban, cơ quan thuộc Tỉnh ủy, các Ban của Hội đồng nhân dân tỉnh, Ủy ban Mặt trận Tổ quốc Việt Nam tỉnh và các tổ chức chính trị - xã hội tỉnh nghiêm túc triển khai thực hiện Công văn này. Trong quá trình tổ chức thực hiện, nếu có khó khăn, vướng mắc, các cơ quan, đơn vị, địa phương kịp thời phản ánh về Công an tỉnh (qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) để được hướng dẫn hoặc tổng hợp, báo cáo Ủy ban nhân dân tỉnh xem xét, chỉ đạo theo thẩm quyền.

(Gửi kèm Công văn số 2656/BCA-A05 ngày 02/6/2026 của Bộ Công an và Phụ lục các nội dung ưu tiên rà soát)./.

Nơi nhận:

- Như trên;
- Thường trực: Tỉnh ủy, HĐND tỉnh;
- Chủ tịch, các Phó Chủ tịch UBND tỉnh;
- Lãnh đạo VP UBND tỉnh;
- Lưu: VT, CVNC^{Tường}.



**KT. CHỦ TỊCH
PHÓ CHỦ TỊCH THƯỜNG TRỰC**



Nguyễn Lê Huy



PHỤ LỤC

Các nội dung ưu tiên rà soát, thực hiện “TCVN 14423:2025 An ninh mạng - Yêu cầu đối với hệ thống thông tin quan trọng”

(Kèm theo Công văn số 4626/UBND-NC ngày 17 tháng 7 năm 2026 của Chủ tịch UBND tỉnh)

STT	Nhiệm vụ	Đơn vị thực hiện	Thời hạn hoàn thành
1	Xác định và phân loại tài sản trong hệ thống thông tin: Thực hiện rà soát, lập danh mục tất cả các tài sản phần cứng, phần mềm, dữ liệu trong hệ thống thông tin. Trong đó, nghiên cứu, đánh giá mức độ quan trọng của từng tài sản làm cơ sở xây dựng và triển khai phương án bảo đảm an ninh mạng cho hệ thống thông tin theo nguyên tắc “bảo vệ đúng, đầu tư đủ”, phân bổ nguồn lực khoa học, tối ưu, tránh gây lãng phí.	Cơ quan, đơn vị, địa phương	Thường xuyên
2	Xác định và chuẩn hóa mô hình hệ thống thông tin: Tiến hành rà soát, cập nhật sơ đồ logic và vật lý của hệ thống thông tin, đảm bảo hệ thống được thiết kế theo nguyên tắc phân chia vùng mạng dựa theo chức năng và tuân thủ nguyên tắc “đặc quyền tối thiểu”, hạn chế tối đa bề mặt tấn công, ngăn chặn rủi ro lây lan khi sự cố xảy ra.	Cơ quan, đơn vị, địa phương	Thường xuyên
3	Cấu hình bảo mật, rà soát, bóc gỡ mã độc và cập nhật bản vá: Thực hiện kiểm tra, đánh giá và cấu hình bảo mật toàn bộ các tài sản trong hệ thống thông tin, thứ tự ưu tiên thực hiện dựa theo mức độ quan trọng của tài sản. Khẩn trương cài đặt đầy đủ phần mềm phòng chống mã độc, rà quét, bóc gỡ triệt để mã độc trong hệ thống thông tin, đồng thời cập nhật các bản vá của hệ điều hành, ứng dụng đối với các lỗ hổng bảo mật đã được công bố.	Cơ quan, đơn vị, địa phương	Thường xuyên
4	Triển khai, kết nối giám sát an ninh mạng: Thiết lập và duy trì giải pháp giám sát an ninh mạng 24/7 đối với toàn bộ lưu	Cơ quan, đơn vị, địa phương	Thường xuyên

	lượng, sự kiện và nhật ký phần cứng, phần mềm trong hệ thống thông tin, đảm bảo khả năng phát hiện sớm, cảnh báo kịp thời các dấu hiệu bất thường, hành vi xâm nhập trái phép tác động tiêu cực đến hệ thống thông tin. Thực hiện kết nối hệ thống giám sát an ninh mạng về Trung tâm An ninh mạng quốc gia (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an) để chia sẻ thông tin cảnh báo, hỗ trợ giám sát an ninh mạng, kịp thời phát hiện, ngăn chặn các mối đe dọa trên không gian mạng.		
5	Rà soát, cập nhật, quy trình, quy định quản lý, vận hành hệ thống thông tin, đảm bảo an ninh mạng, nâng cao năng lực, trình độ của cán bộ, nhân viên quản trị, vận hành, khai thác hệ thống thông tin: Tập trung kiện toàn tổ chức, nhân sự và chính sách nội bộ ¹ , khẩn trương ban hành các quy chế bảo mật, làm rõ quyền hạn, trách nhiệm của từng cá nhân tham gia quản trị, vận hành, khai thác và bảo vệ hệ thống thông tin. Đồng thời, tổ chức đào tạo nâng cao chuyên môn, nhận thức đảm bảo an ninh mạng cho toàn thể cán bộ, nhân viên nhằm hạn chế rủi ro tấn công mạng, lộ lọt dữ liệu xuất phát từ sự thiếu hiểu biết, thiếu tuân thủ chính sách và tính chủ quan của người dùng.	Cơ quan, đơn vị, địa phương	Thường xuyên

¹ Tối thiểu bao gồm: ⁽¹⁾ Các quy định, quy trình quản lý, vận hành, bảo vệ hệ thống thông tin; ⁽²⁾ Quy chế bảo đảm an ninh mạng cho hệ thống thông tin đảm bảo tuân thủ quy định của pháp luật về an ninh mạng.