

**ỦY BAN NHÂN DÂN
TỈNH BẮC NINH**

Số: /UBND-NC

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

Bắc Ninh, ngày tháng 7 năm 2026

V/v triển khai hướng dẫn của Bộ
Công an về công tác bảo đảm an
ninh mạng, an ninh thông tin, an
ninh dữ liệu

Kính gửi:

- Các ban, cơ quan thuộc Tỉnh ủy;
- Các ban, cơ quan thuộc HĐND tỉnh;
- Ủy ban MTTQ Việt Nam tỉnh và các tổ chức thành viên;
- Các Sở, cơ quan thuộc UBND tỉnh;
- UBND các xã, phường.

Thực hiện Công văn số 2656/BCA-A05 ngày 02/6/2026 của Bộ Công an về hướng dẫn triển khai công tác bảo đảm an ninh mạng, an ninh thông tin, an ninh dữ liệu, để bảo đảm an ninh mạng và nâng cao năng lực bảo vệ hệ thống thông tin của các cơ quan nhà nước trên địa bàn tỉnh; Chủ tịch UBND tỉnh có ý kiến như sau:

1. Yêu cầu các Sở, cơ quan thuộc UBND tỉnh, UBND các xã, phường tập trung thực hiện một số nội dung:

- Khẩn trương nghiên cứu, tham chiếu tiêu chuẩn quốc gia “TCVN 14423:2025 An ninh mạng - Yêu cầu đối với hệ thống thông tin quan trọng” làm cơ sở đánh giá tổng thể về an ninh mạng, bảo mật thông tin, an ninh dữ liệu, cập nhật, bổ sung chính sách quản lý, quy trình quản trị, giải pháp bảo đảm an ninh mạng cho các hệ thống thông tin, trong đó ưu tiên rà soát, thực hiện các nội dung tại phụ lục kèm theo Công văn.

- Định kỳ triển khai công tác quản lý rủi ro an ninh mạng nhằm tăng cường khả năng phòng thủ chủ động, thực hiện xác định, đánh giá và triển khai các biện pháp giảm thiểu rủi ro, đồng thời chuẩn bị phương án ứng phó khi rủi ro xảy ra để hạn chế tối đa hậu quả. Chú trọng công tác kiểm tra tuân thủ và cập nhật định kỳ quy định, quy trình hoạt động của bộ phận kỹ thuật, chính sách, quy chế bảo đảm an ninh mạng, quy trình quản trị, vận hành hệ thống, quản lý thay đổi, ứng cứu sự cố; đảm bảo các quy trình, quy định, chính sách được ban hành sát với thực tiễn, có hiệu quả, không mang tính thủ tục, hành chính.

- Nâng cao hiệu quả công tác bảo đảm an ninh dữ liệu, an ninh thông tin, bảo vệ thông tin thuộc phạm vi bí mật nhà nước thông qua việc tuân thủ tuyệt đối quy định của pháp luật¹, trong đó tập trung áp dụng các biện pháp cách ly vật lý, mã hóa cơ yếu và kiểm soát chặt chẽ quyền truy cập, tăng cường quản lý định

¹ Luật An ninh mạng 2025, Luật Bảo vệ bí mật nhà nước 2025, Luật Bảo vệ dữ liệu cá nhân 2025, Luật Dữ liệu 2024 và các văn bản hướng dẫn dưới luật đi kèm.

danh, xác thực người dùng ngăn chặn tình trạng thu thập, khai thác và sử dụng trái phép thông tin công dân.

Đồng thời, cần triển khai cơ chế quản lý, kiểm soát kỹ thuật trong toàn bộ vòng đời của dữ liệu, chú trọng các công tác: (1) Phân loại, xác định và gắn nhãn mức độ mật, nhạy cảm của tài liệu ngay từ khâu tạo lập; (2) Triển khai hệ thống sao lưu dự phòng tách biệt với hệ thống mạng chính, đảm bảo khả năng phục hồi dữ liệu; (3) Áp dụng các giải pháp mã hóa đối với dữ liệu trong quá trình lưu trữ và truyền đưa trên môi trường mạng; (4) Thực hiện nghiêm quy trình xóa dữ liệu an toàn hoặc tiêu hủy thiết bị lưu trữ khi không còn nhu cầu sử dụng theo quy định.

2. Đề nghị các Ban, cơ quan thuộc Tỉnh ủy, HĐND tỉnh, Ủy ban MTTQ Việt Nam tỉnh và các tổ chức chính trị - xã hội tỉnh căn cứ chức năng, nhiệm vụ được giao, phối hợp chỉ đạo và tổ chức triển khai thực hiện các nội dung tại Công văn này và Phụ lục kèm theo đối với các hệ thống thông tin thuộc phạm vi quản lý, bảo đảm đồng bộ, hiệu quả và đúng tiến độ.

3. Các cơ quan, đơn vị, địa phương báo cáo, thông tin kết quả thực hiện về UBND tỉnh (*qua Công an tỉnh*) trước ngày **15/7/2026** để tổng hợp, báo cáo Bộ Công an theo quy định. Trong quá trình triển khai, nếu phát sinh khó khăn, vướng mắc vượt thẩm quyền, kịp thời phản ánh về UBND tỉnh (*qua Công an tỉnh*) để được xem xét, chỉ đạo giải quyết.

4. Giao Công an tỉnh chủ trì, theo dõi, hướng dẫn, đôn đốc các cơ quan, đơn vị, địa phương triển khai thực hiện các nội dung nêu trên; định kỳ tổng hợp tình hình, kết quả thực hiện, tham mưu UBND tỉnh báo cáo Bộ Công an theo quy định.

(*Gửi kèm theo 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;
- TT Tỉnh ủy, TT HĐND tỉnh;
- CT, các PCT UBND tỉnh;
- VP UBND tỉnh: CVP, TH, HCQT;
- Lưu: VT, NC.

**TL. CHỦ TỊCH
CHÁNH VĂN PHÒNG**

Vũ Huy Phương

PHỤ LỤC

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

(Kèm theo Công văn số /UBND-NC ngày 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 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	Công an tỉnh chủ trì, phối hợp Sở Khoa học và Công	Thường xuyên

	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.	nghệ và các cơ quan, đơn vị liên quan	
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.