

**ỦY BAN NHÂN DÂN
TỈNH HƯNG YÊN**

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

Số: /UBND-NC
V/v nâng cao hiệu quả công tác
bảo vệ bí mật nhà nước và
an ninh mạng trên địa bàn tỉnh

Hưng Yên, ngày tháng 3 năm 2026

Kính gửi:

- Các sở, ban, ngành, đoàn thể tỉnh;
- UBND xã, phường.

Năm 2025, qua công tác thanh tra chuyên đề “Việc chấp hành các quy định của pháp luật về bảo vệ bí mật nhà nước và an ninh mạng” trên phạm vi toàn quốc, ngày 27/01/2026, Thanh tra Bộ Công an có Công văn số 261/X05-P5 chỉ ra nhiều tồn tại, hạn chế tại các cơ quan, đơn vị, như:

- Về nghiệp vụ bảo vệ bí mật nhà nước (BMNN): Nhiều văn bản xác định độ mật không đúng thực tế; đóng dấu mật cho văn bản không chứa nội dung bí mật hoặc ngược lại. Phiếu đề xuất độ mật thường thiếu căn cứ pháp lý cụ thể (không ghi rõ điểm, khoản, điều của danh mục BMNN) hoặc phát hành văn bản mật mà không có tờ trình, phiếu trình đề xuất. Còn tình trạng cấp phó ký phát hành văn bản mật không đúng thẩm quyền. Văn bản mật phát hành thiếu thông tin tại ô “Nơi nhận” (số lượng bản, phạm vi sao chụp) và thiếu dấu “Bản số” theo quy định. Công tác bảo quản tài liệu mật tại một số nơi còn lỏng lẻo dẫn đến thất lạc văn bản. Việc sao chụp tài liệu thực hiện sai trình tự, thẩm quyền; quy trình giao nhận không qua đầu mối KT1 và không ký nhận bàn giao tại sổ chuyển giao. Nhiều đơn vị chưa lập đầy đủ các mẫu sổ quản lý hoặc trang bị mẫu dấu không đúng quy định.

- Về công tác an ninh mạng (ANM) và an toàn thông tin: Nhiều hệ thống thông tin chưa phê duyệt cấp độ an toàn hoặc hồ sơ đề xuất không phù hợp hạ tầng thực tế. Giải pháp bảo mật theo cấp độ chưa triển khai đầy đủ, để lộ lỗ hổng và mật khẩu tài khoản đăng nhập trên môi trường mạng. Còn vi phạm quy định khi dùng máy tính kết nối Internet để soạn thảo, lưu trữ tài liệu mật; thiết bị đầu cuối đưa vào sử dụng nhưng không qua kiểm tra an ninh. Máy tính sử dụng hệ điều hành cũ, không bản quyền, không cài phần mềm diệt virus dẫn đến nguy cơ cao bị tấn công mã độc và chiếm quyền điều khiển.

- Về quản lý điều hành và nguồn lực: Chưa ban hành đầy đủ nội quy bảo vệ BMNN và nội quy an ninh mạng theo pháp luật hiện hành. Chưa bố trí cán bộ chuyên trách thực hiện công tác bảo vệ BMNN; công tác tự kiểm tra và chế độ báo cáo định kỳ chưa được thực hiện nghiêm túc. Không lập dự toán hoặc bố trí kinh phí riêng cho công tác bảo vệ BMNN và an ninh mạng.

Để kịp thời chấn chỉnh, không để xảy ra vi phạm tương tự trên địa bàn tỉnh, UBND tỉnh yêu cầu Thủ trưởng các cơ quan, đơn vị tập trung thực hiện các nội dung sau:

1. Tổ chức quán triệt ngay các tồn tại nêu trên để cán bộ, công chức tự đổi chiều, khắc phục, không để xảy ra vi phạm tương tự trong cơ quan, đơn vị phụ trách. Đẩy mạnh tuyên truyền Luật Bảo vệ BMNN năm 2025 và Nghị định số 63/2026/NĐ-CP ngày 28/02/2026 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Bảo vệ BMNN.

2. Chỉ đạo các cơ quan, đơn vị trực thuộc thực hiện nghiêm công tác bảo vệ BMNN và ANM, nâng cao trách nhiệm người đứng đầu các cơ quan, tổ chức và đơn vị, gắn trách nhiệm bảo vệ BMNN và an ninh mạng đối với cá nhân, tập thể trong soạn thảo, lưu trữ, quản lý, vận chuyển, bàn giao, cung cấp BMNN và sử dụng hệ thống thông tin an ninh mạng.

3. Bố trí nguồn lực đầu tư cho cơ sở hạ tầng, trang thiết bị, công cụ, phương tiện về công nghệ thông tin và áp dụng, sử dụng các sản phẩm mật mã, thiết bị cơ yếu phục vụ công tác bảo vệ BMNN và an ninh mạng; tuyển dụng, đào tạo nguồn nhân lực chất lượng cao về công nghệ thông tin, an ninh mạng đáp ứng các nhiệm vụ và kịp thời tham mưu giải quyết, xử lý các sự cố tấn công mạng, an ninh mạng, ngăn chặn nguy cơ lộ, mất BMNN, mất thông tin, dữ liệu của cơ quan, tổ chức, bộ máy hành chính nhà nước. Triển khai đầy đủ các giải pháp bảo đảm an toàn, an ninh mạng, bảo mật, phương án ứng phó sự cố an toàn thông tin mạng đối với các thiết bị đầu cuối, các hệ thống công nghệ thông tin quan trọng, dùng chung; khuyến nghị sử dụng các nền tảng, sản phẩm, dịch vụ an ninh mạng trong nước để nâng cao hiệu quả hoạt động quản lý và thực thi pháp luật về an toàn thông tin, an ninh mạng.

4. Thường xuyên tự kiểm tra công tác bảo vệ BMNN theo quy định tại khoản 2 Điều 25 Luật Bảo vệ BMNN; chủ động phối hợp với Công an tỉnh, Sở Khoa học và Công nghệ, Văn phòng Tỉnh ủy, Văn phòng UBND tỉnh trong xây dựng và triển khai các hoạt động kiểm tra, đánh giá trang thiết bị công nghệ thông tin về an toàn, an ninh mạng, bảo mật thông tin, dữ liệu; chấp hành nghiêm túc chế độ báo cáo định kỳ, đột xuất về công tác bảo vệ BMNN theo quy định.

5. Các cơ quan, đơn vị có hoạt động thu thập, xử lý dữ liệu cá nhân tiến hành rà soát tổng thể, phân loại dữ liệu cá nhân đã thu thập, đang xử lý; xác định trách nhiệm bảo vệ tương ứng với từng loại dữ liệu cá nhân theo đúng quy định tại Luật Dữ liệu, Luật Bảo vệ dữ liệu cá nhân. Rà soát, đánh giá quy trình thu thập, xử lý dữ liệu cá nhân, đề xuất các biện pháp quản lý phù hợp với quy mô, mức độ xử lý dữ liệu cá nhân của cơ quan, đơn vị; chỉ định bộ phận chuyên trách có chức năng bảo vệ dữ liệu cá nhân của cơ quan, đơn vị. Đối với cơ quan, đơn vị đang xử lý khối lượng lớn dữ liệu cá nhân cần thường xuyên kiểm tra, đánh giá đảm bảo an ninh, an toàn thông tin trong hoạt động xử lý.

6. Giao Công an tỉnh chủ trì, phối hợp các cơ quan, đơn vị liên quan thường xuyên rà soát tham mưu kiện toàn Tiểu Ban an ninh mạng, Ban Chỉ đạo công tác bảo vệ BMNN cấp tỉnh. Tổ chức các lớp tập huấn chuyên sâu về công tác bảo vệ BMNN, nâng cao kiến thức về an ninh mạng và an toàn thông tin mạng cho cán bộ, công chức, viên chức được giao kiêm nhiệm thực hiện công tác bảo vệ BMNN và an ninh mạng tại các cơ quan, đơn vị trên địa bàn tỉnh. Tăng cường công tác thanh tra, kiểm tra, hướng dẫn đối với cơ quan, tổ chức và phát hiện, xử lý các hành vi vi phạm về bảo vệ BMNN và an ninh mạng theo thẩm quyền. Phối hợp với Sở Khoa học và Công nghệ, Văn phòng Tỉnh ủy, Văn phòng UBND tỉnh tham mưu Bí thư Tỉnh ủy, Chủ tịch UBND tỉnh thực hiện triển khai mô hình bảo đảm an toàn thông tin “4 lớp” đối với hệ thống thông tin các cơ quan Đảng, Nhà nước, tổ chức chính trị - xã hội trên địa bàn tỉnh; hướng dẫn các cơ quan, tổ chức áp dụng Tiêu chuẩn quốc gia TCVN 11930:2017 và TCVN 14423:2025, trong đó tập trung hướng dẫn triển khai quản lý rủi ro an ninh mạng (theo hướng dẫn của Bộ Công an). Hướng dẫn, kiểm tra, đôn đốc các cơ quan, đơn vị, địa phương triển khai thực hiện; tổng hợp kết quả, báo cáo Bộ Công an và UBND tỉnh theo quy định./.

Nơi nhận:

- Như trên;
- Bộ Công an (X05; A03, A05);
- Thường trực Tỉnh ủy;
- Chủ tịch, các PCT UBND tỉnh;
- Công an tỉnh;
- LĐVP UBND tỉnh;
- Lưu: VT, CVNC^{Tưong}.

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

Nguyễn Lê Huy