

Số: 1894 /UBND-VP

Mỹ Hào, ngày 20 tháng 7 năm 2026

V/v triển khai thực hiện Công văn số
4626/UBND-NC ngày 17/7/2026 của
UBND tỉnh Hưng Yên về bảo đảm an ninh
mạng, an ninh thông tin và an ninh dữ liệu

Kính gửi:

- Các phòng, ban, ngành, đoàn thể phường;
- Công an phường;
- Trung tâm Phục vụ hành chính công phường;
- Trung tâm Dịch vụ tổng hợp phường;
- Các tổ dân phố.

Thực hiện Công văn số 4626/UBND-NC ngày 17/7/2026 của UBND tỉnh Hưng Yên về bảo đảm an ninh mạng, an ninh thông tin và an ninh dữ liệu; nhằm 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; bảo đảm hoạt động thông suốt, an toàn của các hệ thống thông tin phục vụ công tác lãnh đạo, chỉ đạo, điều hành và giải quyết thủ tục hành chính trên địa bàn phường; UBND phường yêu cầu các phòng chuyên môn, các cơ quan, đơn vị và tổ dân phố nghiêm túc triển khai thực hiện các nội dung sau:

1. Tổ chức quán triệt, triển khai thực hiện nghiêm các quy định của pháp luật về bảo đảm an ninh mạng, an ninh thông tin và an ninh dữ liệu

- Tổ chức quán triệt, triển khai thực hiện nghiêm các quy định của pháp luật về an ninh mạng, an toàn thông tin mạng, bảo vệ dữ liệu, bảo vệ bí mật nhà nước và các văn bản hướng dẫn của Bộ Công an và các văn bản chỉ đạo của UBND tỉnh, Công an tỉnh về công tác bảo đảm an ninh mạng, an ninh thông tin và an ninh dữ liệu đến toàn thể cán bộ, công chức, viên chức, người lao động thuộc phạm vi quản lý; nâng cao trách nhiệm của người đứng đầu và của từng cán bộ, công chức, viên chức, người lao động trong quản lý, khai thác, sử dụng hệ thống thông tin, bảo vệ dữ liệu, dữ liệu cá nhân và bí mật nhà nước.

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 số 4626/UBND-NC ngày 17/7/2026 của UBND tỉnh Hưng Yên (gửi kèm) phù hợp với điều kiện thực tế của cơ quan, đơn vị.

2. Rà soát, đánh giá công tác bảo đảm an ninh mạng, an ninh thông tin và an ninh dữ liệu

- Tổ chức 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 phát hiện, 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 và bảo đảm an ninh mạng theo quy định.

- Chủ động triển khai các nội dung ưu tiên rà soát, thực hiện theo Phụ lục kèm theo Công văn số 4626/UBND-NC ngày 17/7/2026 của UBND tỉnh Hưng Yên; trong đó tập trung rà soát, lập danh mục, phân loại tài sản của hệ thống thông tin; rà soát, cập nhật, chuẩn hóa mô hình hệ thống thông tin; kiểm tra, cấu hình bảo mật, cài đặt phần mềm phòng, chống mã độc, thực hiện rà quét, bóc gỡ mã độc (nếu có), cập nhật các bản vá bảo mật đã được công bố; rà soát, bổ sung, hoàn thiện quy trình quản lý, vận hành hệ thống thông tin, sao lưu, phục hồi dữ liệu, phương án ứng phó, khắc phục sự cố an ninh mạng; bảo đảm việc quản lý, vận hành hệ thống thông tin an toàn, liên tục, hiệu quả theo quy định.

3. Tăng cường công tác quản lý rủi ro, giám sát an ninh mạng và bảo vệ dữ liệu

- Triển khai đầy đủ các biện pháp phòng ngừa, phát hiện, ngăn chặn, ứng phó, 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.

- Thường xuyên theo dõi, kiểm tra việc thực hiện các biện pháp bảo đảm an ninh mạng, an ninh thông tin và an ninh dữ liệu; chủ động phòng ngừa, phát hiện, cảnh báo, ngăn chặn và xử lý kịp thời các nguy cơ, sự cố phát sinh, bảo đảm hoạt động an toàn, liên tục của các hệ thống thông tin thuộc phạm vi quản lý.

4. Nâng cao trách nhiệm của người đứng đầu

Người đứng đầu các cơ quan, đơn vị thuộc phạm vi quản lý của UBND phường chịu trách nhiệm trước Chủ tịch UBND phường 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.

5. Tổ chức tự kiểm tra, đánh giá

Định kỳ hoặc khi có yêu cầu, các cơ quan, đơn vị chủ động 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; phối hợp với cơ quan Công an và các cơ quan có thẩm quyền trong công tác kiểm tra, hướng dẫn, xử lý các sự cố an ninh mạng theo quy định.

6. Tổ chức thực hiện

- Giao Công an phường chủ trì theo dõi, nắm tình hình liên quan đến an ninh mạng, an ninh thông tin và an ninh dữ liệu trên địa bàn; tham mưu UBND phường chỉ đạo triển khai các quy định, biện pháp bảo đảm an ninh mạng, an ninh thông tin và an ninh dữ liệu theo chức năng, nhiệm vụ được giao; phối hợp với Văn phòng HĐND và UBND phường, các phòng chuyên môn, cơ quan, đơn vị có liên quan đôn đốc việc triển khai thực hiện Công văn này; kịp thời phát hiện, tổng hợp, báo cáo UBND phường các nguy cơ, lỗ hổng, điểm yếu, dấu hiệu mất an ninh mạng, an ninh thông tin, lộ, lọt dữ liệu hoặc sự cố an ninh mạng; đồng thời phối hợp với Công an tỉnh trong công tác kiểm tra, hướng dẫn, xử lý, ứng phó và khắc phục sự cố an ninh mạng theo quy định.

- Văn phòng HĐND và UBND phường theo dõi, đôn đốc, tổng hợp tình hình triển khai thực hiện Công văn; tham mưu UBND phường chỉ đạo, kiểm tra việc thực hiện; tổng hợp các khó khăn, vướng mắc, báo cáo cơ quan có thẩm quyền theo quy định.

Yêu cầu các phòng chuyên môn, các cơ quan, đơn vị và tổ dân phố nghiêm túc triển khai thực hiện Công văn này. Trong quá trình tổ chức thực hiện, nếu có khó khăn, vướng mắc, kịp thời phản ánh về UBND phường (qua Văn phòng HĐND và UBND phường) để tổng hợp, tham mưu báo cáo cơ quan có thẩm quyền xem xét, hướng dẫn, giải quyết theo quy định. /

Nơi nhận:

- Như trên;
- Thường trực Đảng ủy phường;
- Thường trực HĐND phường;
- Lãnh đạo UBND phường;
- Lưu: VT.



Nguyễn Thế Thành