

**ỦY BAN NHÂN DÂN
PHƯỜNG HÀ TU**

Số: 1201/UBND-VHXXH

V/v cảnh báo nguy cơ mất an toàn thông tin,
an ninh mạng khi sử dụng các công cụ trí tuệ
nhân tạo (AI)

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

Hà Tu, ngày 18 tháng 11 năm 2025

Kính gửi: Các phòng ban, đơn vị trực thuộc.

Trong bối cảnh chuyển đổi số đang diễn ra mạnh mẽ, việc ứng dụng trí tuệ nhân tạo (AI) đã trở thành xu thế phổ biến tất yếu, được nhiều cơ quan, đơn vị, cán bộ, công chức, viên chức chủ động khai thác, sử dụng để nâng cao hiệu quả công việc. Các công cụ AI phổ biến có nguồn gốc từ nước ngoài như ChatGPT, Gemini (Hoa Kỳ), Manus (Trung Quốc),... mang lại nhiều tiện ích trong việc tìm kiếm, tra cứu văn bản pháp luật, tổng hợp thông tin, soạn thảo công văn, báo cáo, tóm tắt, dịch thuật văn bản,... Tuy nhiên, việc sử dụng các công cụ AI chưa qua kiểm duyệt, đặc biệt là các nền tảng có máy chủ đặt tại nước ngoài gây ra nguy cơ về việc lộ, lọt thông tin, dữ liệu, tài liệu nội bộ và bí mật nhà nước (BMNN). Các hệ thống AI này có thể thu thập, sử dụng, phân tích dữ liệu, chia sẻ dữ liệu cho bên thứ ba, cơ quan tình báo nước ngoài có thể thu thập được các tài liệu từ các nền tảng, gây ra hậu quả nghiêm trọng đến công tác bảo đảm an ninh quốc gia, an toàn thông tin của các cơ quan trên địa bàn tỉnh.

Thực hiện Công văn số 4383/UBND-VHXXH ngày 18/11/2025 của Ủy ban nhân dân tỉnh về việc cảnh báo nguy cơ mất an toàn thông tin, an ninh mạng khi sử dụng các công cụ trí tuệ nhân tạo (AI). Ủy ban nhân dân phường có ý kiến chỉ đạo như sau:

1. Các phòng ban, đơn vị trực thuộc UBND phường nghiêm túc quán triệt đến toàn thể cán bộ, công chức, viên chức, người lao động cảnh giác, không thực hiện việc chia sẻ thông tin nguồn trong việc sử dụng trí tuệ nhân tạo AI có thể gây ra nguy cơ mất đảm bảo an toàn thông tin, an ninh mạng, nhất là trong các trường hợp sau:

(1) Tải các văn bản, tài liệu, bản ghi âm thanh, nội dung ghi âm cuộc họp (để chuyển sang định dạng văng bản) có chứa nội dung nội bộ, tài liệu BMNN lên các nền tảng AI để nhờ hỗ trợ soạn thảo, tóm tắt, phân tích và dịch thuật văn bản, dẫn đến nguy cơ thông tin, dữ liệu của cơ quan, đơn vị bị rò rỉ ra bên ngoài, bị các hệ thống AI thu thập hoặc khai thác trái phép.

(2) Sử dụng công cụ AI để xử lý hình ảnh, trích xuất nội dung từ ảnh chụp bản báo cáo, hồ sơ có đính kèm thông tin nhạy cảm (ảnh chân dung, số điện thoại, chức vụ, địa chỉ email, thông tin người thân...). Những dữ liệu này có thể bị hệ thống AI lưu trữ, tái sử dụng hoặc bị lộ, lọt ra ngoài dưới dạng gợi ý cho những tổ chức, cá nhân khác khai thác, sử dụng trái phép.

(3) Đưa những văn bản có những nội dung, dữ liệu của tỉnh lên nền tảng AI có máy chủ đặt tại nước ngoài để xây dựng các kế hoạch, chương trình về phát triển kinh tế xã hội của tỉnh, của phường là những nguy cơ để các cơ quan đặc biệt nước ngoài lợi dụng sẽ thu thập thông tin tình báo.

(4) Nhập thông tin về danh sách, lịch trình di chuyển, kế hoạch công tác của các đồng chí Lãnh đạo hoặc các đoàn công tác vào AI để nhờ hỗ trợ sắp xếp, lên kế hoạch. Việc này có thể làm lộ thông tin về hành trình, nhân sự, phương tiện, địa điểm, các tổ chức khủng bố hoặc cơ quan tình báo nước ngoài có thể thu thập được, gây ra ảnh hưởng nghiêm trọng đến an ninh quốc gia.

2. Để chủ động phòng ngừa, ngăn chặn có hiệu quả các nguy cơ trên, bảo đảm an toàn hệ thống thông tin, cơ sở dữ liệu, bảo vệ BMNN, dữ liệu nội bộ và an ninh quốc gia, UBND phường giao Thủ trưởng các phòng ban, đơn vị:

- Tăng cường phổ biến, quán triệt đến toàn thể cán bộ, công chức, viên chức, người lao động tại cơ quan, đơn vị về các quy định của pháp luật trong công tác bảo vệ BMNN, các nguy cơ, rủi ro và hậu quả của việc làm lộ, lọt thông tin khi sử dụng các công cụ trí tuệ nhân tạo AI trên không gian mạng. Nâng cao nhận thức, trách nhiệm của mỗi cá nhân trong việc bảo vệ dữ liệu nội bộ, thông tin cá nhân và BMNN trên không gian mạng.

- Tổ chức tự kiểm tra, rà soát việc sử dụng các công cụ, phần mềm trí tuệ nhân tạo AI trong hoạt động của cơ quan, đơn vị. Kịp thời chấn chỉnh, xử lý nghiêm các trường hợp tải nội dung nhạy cảm, tài liệu nội bộ, BMNN lên nền tảng trí tuệ nhân tạo.

Ủy ban nhân dân phường Hà Tu giao Thủ trưởng các phòng ban, đơn vị nghiêm túc chỉ đạo, thực hiện./. *Handwritten signature*

Nơi nhận:

- Như trên (thực hiện);
- CT, các PCT UBND (chỉ đạo);
- Các CQTMGV Đảng ủy (phối hợp);
- Phòng VHXH;
- Lưu VT.

Handwritten signature

**KT. CHỦ TỊCH
PHÓ CHỦ TỊCH**



Vũ Đức Cường