

Số: 2547 /UBND-CA

Mỹ Hào, ngày 14 tháng 9 năm 2026

V/v tăng cường công tác bảo đảm
an toàn thông tin, an ninh mạng
trong các cơ quan, đơn vị và trên
địa bàn phường

Kính gửi:

- Công an phường;
- Các phòng, ban, ngành, đoàn thể phường;
- Bí thư Chi bộ, Tổ trưởng các tổ dân phố;
- Tổ công nghệ số cộng đồng các tổ dân phố.

Căn cứ Luật An toàn thông tin mạng năm 2015; Luật An ninh mạng năm 2018; Nghị quyết số 57-NQ/TW ngày 22/12/2024 của Bộ Chính trị về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia và các quy định có liên quan;

Thời gian qua, công tác chuyển đổi số, ứng dụng công nghệ thông tin, khai thác các hệ thống thông tin và cung cấp dịch vụ công trực tuyến phục vụ người dân, doanh nghiệp trên địa bàn phường được quan tâm triển khai và đạt nhiều kết quả tích cực. Tuy nhiên, cùng với quá trình đẩy mạnh ứng dụng công nghệ số, các nguy cơ mất an toàn thông tin, mất an ninh mạng ngày càng diễn biến phức tạp; nguy cơ mã độc xâm nhập, tấn công hệ thống thông tin; lộ, mất, rò rỉ dữ liệu cá nhân, thông tin nội bộ và các thông tin thuộc phạm vi cần bảo vệ trên môi trường mạng; các hoạt động lừa đảo, chiếm đoạt tài sản trên không gian mạng với phương thức, thủ đoạn ngày càng tinh vi vẫn tiềm ẩn nhiều nguy cơ. Trong khi đó, nhận thức, ý thức cảnh giác và kỹ năng bảo đảm an toàn thông tin của một bộ phận cán bộ, công chức và Nhân dân còn hạn chế.

Nhằm chủ động phòng ngừa, phát hiện, ngăn chặn và xử lý kịp thời các nguy cơ, sự cố mất an toàn thông tin, bảo đảm an toàn đối với hệ thống thông tin, dữ liệu và hoạt động của cơ quan trên môi trường mạng; nâng cao nhận thức, kỹ năng tự bảo vệ thông tin cho cán bộ, công chức và Nhân dân, Ủy ban nhân dân phường yêu cầu các phòng chuyên môn thuộc UBND phường, các cơ quan, đơn vị có liên quan, tổ dân phố và toàn thể cán bộ, công chức nghiêm túc triển khai thực hiện các nội dung sau:

1. Đối với cán bộ, công chức, người lao động thuộc cơ quan UBND phường

a) Nâng cao ý thức, trách nhiệm và kỷ luật bảo mật

- Chấp hành nghiêm các quy định của pháp luật và của cơ quan về an toàn thông tin mạng, an ninh mạng, bảo vệ dữ liệu cá nhân và bảo vệ bí mật nhà nước. Không tự ý sao chép, lưu trữ, gửi, chia sẻ tài liệu thuộc phạm vi bí mật nhà nước, thông tin nội bộ hoặc dữ liệu công vụ trên thiết bị cá nhân, tài khoản cá nhân, dịch vụ lưu trữ trực tuyến hoặc các nền tảng trao đổi thông tin không được cơ quan cho phép.

- Không sử dụng thư điện tử cá nhân, tài khoản mạng xã hội hoặc các nền tảng trực tuyến không được phép để trao đổi, truyền nhận tài liệu, dữ liệu công vụ có nội dung cần bảo mật.

- Khi phát hiện dấu hiệu nghi ngờ lộ, mất dữ liệu, tài khoản bị chiếm quyền sử dụng hoặc có sự cố an toàn thông tin, phải kịp thời báo cáo người phụ trách và Văn phòng HĐND và UBND phường để phối hợp xử lý; không tự ý xử lý làm thay đổi hiện trạng hoặc xóa dữ liệu liên quan đến sự cố.

b) Quản lý thiết bị và phương tiện kết nối

- Không tự ý kết nối máy tính, thiết bị công nghệ thông tin của cơ quan với thiết bị lưu trữ cá nhân hoặc thiết bị không rõ nguồn gốc, chưa được kiểm tra an toàn; không tự ý sử dụng USB, thẻ nhớ, ổ cứng di động và các thiết bị lưu trữ ngoài để sao chép dữ liệu công vụ khi chưa được phép.

- Không tự ý kết nối điện thoại, máy tính bảng hoặc thiết bị cá nhân với máy tính của cơ quan để truyền, nhận, sao chép dữ liệu khi chưa được phép và kiểm soát theo quy định.

- Không tự ý tải, cài đặt hoặc sử dụng phần mềm không rõ nguồn gốc, phần mềm bẻ khóa (crack), phần mềm điều khiển máy tính từ xa hoặc các tiện ích có nguy cơ gây mất an toàn thông tin trên máy tính, thiết bị của cơ quan. Việc cài đặt phần mềm phục vụ công việc phải thực hiện theo nhu cầu công vụ và được kiểm soát, phê duyệt theo quy định của cơ quan.

- Không tự ý vô hiệu hóa, thay đổi hoặc can thiệp vào các thiết lập bảo mật, phần mềm phòng, chống mã độc, cấu hình mạng và các biện pháp bảo vệ an toàn thông tin đã được cơ quan thiết lập.

c) Bảo mật tài khoản công vụ và chữ ký số

- Tự quản lý, bảo mật tài khoản và mật khẩu của thư điện tử công vụ, Hệ thống Quản lý văn bản và điều hành, Cổng Dịch vụ công và các hệ thống thông tin được giao sử dụng; không cung cấp, chia sẻ mật khẩu, mã xác thực hoặc thông tin đăng nhập cho người khác sử dụng, trừ trường hợp được thực hiện theo cơ chế quản trị tài khoản của hệ thống.

- Sử dụng mật khẩu có độ dài, độ phức tạp phù hợp; thực hiện thay đổi mật khẩu khi có yêu cầu của hệ thống, cơ quan quản lý hoặc khi phát hiện nguy cơ mất an toàn. Không sử dụng một mật khẩu cho nhiều tài khoản quan trọng; không lưu mật khẩu tại nơi dễ bị người khác tiếp cận.

- Quản lý, bảo quản an toàn thiết bị Token/chứng thư số được cấp; không cho người khác mượn, sử dụng Token hoặc cung cấp mã PIN chữ ký số. Rút Token khỏi

máy tính ngay sau khi hoàn thành việc ký số hoặc khi rời khỏi vị trí làm việc; không để Token kết nối với máy tính khi không trực tiếp sử dụng.

- Khi phát hiện mất Token, lộ mã PIN, nghi ngờ tài khoản hoặc chữ ký số bị sử dụng trái phép, phải báo cáo ngay cho người có thẩm quyền và đầu mối phụ trách công nghệ thông tin của cơ quan để kịp thời khóa, thu hồi hoặc xử lý theo quy định.

2. Công an phường Mỹ Hòa

a) Chủ trì, phối hợp với Văn phòng HĐND và UBND phường và các cơ quan, đơn vị có liên quan tham mưu UBND phường triển khai các biện pháp bảo đảm an ninh mạng; phòng ngừa, phát hiện, đấu tranh, ngăn chặn các hành vi vi phạm pháp luật, tội phạm sử dụng công nghệ cao và các nguy cơ gây mất an ninh, an toàn trên không gian mạng theo chức năng, nhiệm vụ và thẩm quyền.

b) Phối hợp với Văn phòng HĐND và UBND phường kiểm tra, rà soát khi cần thiết hoặc theo yêu cầu đối với việc chấp hành các quy định về an ninh mạng, bảo vệ dữ liệu và sử dụng thiết bị công nghệ thông tin tại Trung tâm Phục vụ hành chính công, các phòng chuyên môn thuộc UBND phường và các đơn vị có liên quan; kịp thời phát hiện, cảnh báo nguy cơ mất an toàn, dấu hiệu mã độc, truy cập trái phép hoặc các hành vi có nguy cơ ảnh hưởng đến an ninh mạng; kiến nghị cơ quan, đơn vị quản lý, vận hành hệ thống thực hiện biện pháp khắc phục, xử lý theo quy định.

c) Chủ động nắm tình hình, phát hiện, đấu tranh, ngăn chặn các hoạt động lừa đảo, chiếm đoạt tài sản, phát tán mã độc, thu thập, đánh cắp thông tin, dữ liệu trái phép và các hành vi vi phạm pháp luật khác trên không gian mạng có liên quan đến địa bàn; tiếp nhận, xác minh, xử lý hoặc tham mưu xử lý theo thẩm quyền đối với các vụ việc phát sinh; trường hợp vượt thẩm quyền thì kịp thời báo cáo, phối hợp với cơ quan chức năng có thẩm quyền giải quyết.

d) Chủ trì cung cấp, biên soạn hoặc phối hợp biên soạn các nội dung cảnh báo về phương thức, thủ đoạn hoạt động của tội phạm, hành vi lừa đảo trên không gian mạng và các khuyến cáo về kỹ năng phòng ngừa để Văn phòng HĐND và UBND phường phối hợp với các cơ quan, đơn vị có liên quan, hệ thống truyền thanh và tổ dân phố tổ chức tuyên truyền đến cán bộ, công chức và Nhân dân trên địa bàn.

đ) Khi phát hiện sự cố hoặc nguy cơ mất an ninh, an toàn thông tin có dấu hiệu liên quan đến tội phạm hoặc hành vi vi phạm pháp luật, chủ động phối hợp với Văn phòng HĐND và UBND phường và đơn vị quản lý, vận hành hệ thống để bảo vệ hiện trường, thu thập thông tin, dữ liệu liên quan và thực hiện các biện pháp xử lý theo quy định; không tự ý can thiệp làm thay đổi, mất dữ liệu hoặc hiện trạng hệ thống khi chưa có yêu cầu của cơ quan có thẩm quyền.

3. Văn phòng HĐND và UBND phường

a) Là đầu mối tham mưu UBND phường trong công tác bảo đảm an toàn thông tin đối với hệ thống thông tin, hạ tầng kỹ thuật, thiết bị công nghệ thông tin

và các tài khoản phục vụ hoạt động của cơ quan. Chủ trì, phối hợp với Công an phường và các đơn vị có liên quan rà soát tổng thể hiện trạng hạ tầng mạng nội bộ (LAN), đường truyền Internet, thiết bị mạng, máy chủ, máy tính và các thiết bị công nghệ thông tin đang được sử dụng tại trụ sở UBND phường; lập danh mục các nguy cơ, điểm yếu cần khắc phục và đề xuất biện pháp xử lý theo thẩm quyền.

b) Rà soát, tham mưu tổ chức phân tách mạng phục vụ hoạt động nghiệp vụ của cơ quan với mạng Wi-Fi phục vụ người dân, khách đến giao dịch và các thiết bị kết nối không thuộc hệ thống nghiệp vụ; bảo đảm thiết bị, tài khoản và dữ liệu phục vụ công việc của cơ quan không bị truy cập trái phép từ các mạng, thiết bị không được kiểm soát.

c) Rà soát tình trạng cài đặt, cập nhật và vận hành các giải pháp phòng, chống mã độc trên máy tính của cơ quan; tham mưu triển khai giải pháp bảo vệ phù hợp, bảo đảm các máy tính thuộc phạm vi quản lý và có kết nối mạng được cài đặt, cập nhật và duy trì giải pháp phòng, chống mã độc theo yêu cầu kỹ thuật và quy định hiện hành.

d) Theo dõi, tiếp nhận và tổng hợp thông tin về các nguy cơ, cảnh báo, sự cố mất an toàn thông tin; phối hợp với Công an phường, đơn vị cung cấp dịch vụ, đơn vị quản trị hệ thống và các phòng chuyên môn có liên quan kiểm tra, cô lập, khắc phục hoặc đề xuất xử lý khi phát hiện thiết bị nhiễm mã độc, tài khoản có dấu hiệu bị xâm nhập hoặc hệ thống có nguy cơ mất an toàn. Thực hiện ghi nhận, tổng hợp và báo cáo kết quả xử lý các sự cố theo quy định.

đ) Trên cơ sở kết quả rà soát, kiểm kê hiện trạng, tham mưu UBND phường xây dựng kế hoạch bảo trì, bảo dưỡng, nâng cấp, thay thế thiết bị mạng, máy chủ, máy tính và các thiết bị công nghệ thông tin không còn đáp ứng yêu cầu kỹ thuật, hiệu năng hoặc an toàn thông tin; phối hợp với cơ quan chuyên môn tham mưu lập dự toán, xác định nguồn kinh phí và trình cấp có thẩm quyền xem xét, quyết định theo quy định của pháp luật về ngân sách nhà nước và đầu tư, mua sắm.

e) Hướng dẫn, đôn đốc cán bộ, công chức, người lao động thực hiện các quy định về quản lý thiết bị, tài khoản, mật khẩu, chữ ký số, dữ liệu và sử dụng các hệ thống thông tin của cơ quan; tổng hợp tình hình, kết quả thực hiện và kịp thời báo cáo Chủ tịch UBND phường những vấn đề phát sinh, nguy cơ mất an toàn thông tin cần chỉ đạo xử lý.

4. Trung tâm Dịch vụ tổng hợp phường

a) Chủ trì công tác thông tin, tuyên truyền trên hệ thống truyền thanh và các kênh thông tin phù hợp của phường; tăng cường tần suất, thời lượng và nội dung tuyên truyền về an toàn thông tin mạng, an ninh mạng, bảo vệ dữ liệu cá nhân và các quy định có liên quan; tuyên truyền các nội dung trọng tâm của Nghị quyết số 57-NQ/TW ngày 22/12/2024 của Bộ Chính trị về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia.

b) Phối hợp với Công an phường và các phòng chuyên môn thuộc UBND phường biên tập, xây dựng nội dung cảnh báo, hướng dẫn Nhân dân nhận diện và phòng tránh các phương thức, thủ đoạn lừa đảo phổ biến trên không gian mạng, như: giả danh cơ quan Công an, Tòa án, Viện kiểm sát; giả danh cán bộ thuế, nhân viên ngân hàng; thông báo trúng thưởng, nhận quà; dụ dỗ cài đặt ứng dụng giả mạo, ứng dụng không rõ nguồn gốc, trong đó có thủ đoạn giả mạo ứng dụng VNeID.

c) Tăng cường tuyên truyền, hướng dẫn người dân các kỹ năng cơ bản để tự bảo vệ dữ liệu cá nhân, tài khoản trực tuyến, tài khoản ngân hàng; không cung cấp mật khẩu, mã OTP, mã xác thực, thông tin tài khoản, thông tin thẻ và các thông tin cá nhân cho người khác qua điện thoại, tin nhắn hoặc các nền tảng trực tuyến khi chưa xác minh rõ danh tính và mục đích sử dụng.

d) Kịp thời tiếp nhận, biên tập và phát hành các nội dung cảnh báo về nguy cơ, phương thức, thủ đoạn lừa đảo, mã độc và các hành vi vi phạm pháp luật trên không gian mạng do Công an phường, các cơ quan chuyên môn và cơ quan có thẩm quyền cung cấp; bảo đảm nội dung tuyên truyền chính xác, dễ hiểu, phù hợp với từng nhóm đối tượng và không làm lộ thông tin thuộc phạm vi cần bảo vệ.

5. Đề nghị Ủy ban MTTQ Việt Nam và các tổ chức chính trị - xã hội phường

a) Phối hợp đẩy mạnh công tác tuyên truyền, vận động đoàn viên, hội viên và Nhân dân nâng cao nhận thức, ý thức chấp hành các quy định về an toàn thông tin mạng, an ninh mạng; chủ động phòng ngừa các nguy cơ mất an toàn thông tin và các hành vi lừa đảo trên không gian mạng.

b) Phát huy vai trò của đoàn viên, hội viên, lực lượng nòng cốt của các tổ chức chính trị - xã hội và phối hợp với các Tổ công nghệ số cộng đồng trong hướng dẫn Nhân dân sử dụng Internet, mạng xã hội và dịch vụ công trực tuyến an toàn, văn minh; cảnh giác với các đường link, cuộc gọi, tin nhắn, tài khoản và ứng dụng không rõ nguồn gốc; không cung cấp mật khẩu, mã OTP, mã xác thực, thông tin tài khoản ngân hàng và dữ liệu cá nhân cho các đối tượng chưa được xác minh.

c) Phối hợp tuyên truyền, vận động Nhân dân không đăng tải, chia sẻ, phát tán thông tin chưa được kiểm chứng; kịp thời thông tin, phản ánh cho Công an phường hoặc cơ quan có thẩm quyền khi phát hiện dấu hiệu lừa đảo, chiếm đoạt tài sản, đánh cắp thông tin, phát tán mã độc hoặc các hành vi vi phạm pháp luật trên không gian mạng.

6. Tổ trưởng các tổ dân phố

a) Tổ chức tuyên truyền, phổ biến nội dung Công văn này và các nội dung cảnh báo về an toàn thông tin, an ninh mạng đến Nhân dân trên địa bàn bằng hình thức phù hợp; lồng ghép trong các cuộc họp tổ dân phố và các hoạt động tuyên truyền tại khu dân cư.

b) Thông tin, chia sẻ kịp thời các nội dung cảnh báo, hướng dẫn nhận diện phương thức, thủ đoạn lừa đảo trên không gian mạng do Công an phường và cơ

quan có thẩm quyền cung cấp trên các nhóm Zalo cộng đồng của khu dân cư, bảo đảm thông tin được kiểm chứng, chính xác.

c) Vận động Nhân dân khi phát hiện dấu hiệu lừa đảo, chiếm đoạt tài sản qua mạng hoặc nghi ngờ thông tin cá nhân, tài khoản bị lộ, mất, chiếm đoạt hoặc sử dụng trái phép thì kịp thời thông báo cho Cảnh sát khu vực hoặc Công an phường để được tiếp nhận, hướng dẫn và xử lý theo quy định.

Ủy ban nhân dân phường yêu cầu các phòng chuyên môn thuộc UBND phường, các cơ quan, đơn vị có liên quan, các tổ dân phố và toàn thể cán bộ, công chức, người lao động nghiêm túc triển khai thực hiện Công văn này./.

Nơi nhận:

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

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH



Ký bởi: ỦY BAN NHÂN DÂN PHƯỜNG
CHỦ TỊCH
Cơ quan: ỦY BAN NHÂN DÂN TỈNH
HUNG YÊN
Thời gian ký: 14/09/2026 14:01:10

Nguyễn Minh Tuấn