UỶ BAN NHÂN DÂN **PHƯỜNG THÁI HÒA**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 441 /UBND-CA V/v tăng cường công tác bảo đảm an toàn thông tin, an ninh mạng trên địa bàn	*Thái Hòa, ngày 24 tháng 9 năm 2025*

Kính gửi: Trưởng các phòng, ban, ngành, đoàn thể phường.

Trong thời gian qua, tỉnh Nghệ An nói chung, phường Thái Hòa nói riêng đã triển khai đẩy mạnh ứng dụng công nghệ thông tin (CNTT) xây dựng chính quyền điện tử, đô thị thông minh tiến tới xây dựng chính quyền số, kinh tế số, xã hội số gắn với bảo đảm an toàn, an ninh mạng. Để đảm bảo các hệ thống ứng dụng CNTT hoạt động tốt trên mạng Internet, đảm bảo an toàn, an ninh mạng, UBND tỉnh đã ban hành nhiều văn bản chỉ đạo; các cơ quan chuyên môn đã hướng dẫn, triển khai nhiều biện pháp, giải pháp kỹ thuật; đầu tư xây dựng các hệ thống đảm bảo an toàn thông tin (ATTT) cho Cổng thông tin điện tử, Hệ thống thư điện tử công vụ; Hệ thống giao ban điện tử trực tuyến; Các hệ thống phần mềm như: phần mềm quản lý văn bản và điều hành VNPTiOffice; Trục kết nối liên thông, Hệ thống một cửa điện tử tích hợp Cổng dịch vụ công trực tuyến thuê dịch vụ của VNPT được đảm bảo bởi hệ thống ATTT của tập đoàn VNPT, đồng thời đa số các cơ quan quản lý nhà nước đã bước đầu quan tâm thực hiện theo các quy định của pháp luật nhằm đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng CNTT trên địa bàn tỉnh vì vậy các hệ thống thông tin, các phần mềm dùng chung, phần mềm chuyên ngành, phần mềm ứng dụng nội bộ tại các cơ quan, đơn vị, địa phương cơ bản được đảm bảo an toàn, an ninh thông tin.

Tuy nhiên, thực tế trên địa bàn phường vẫn còn tình trạng một số cơ quan, đơn vị, tổ chức, cá nhân chưa nhận thức đầy đủ về công tác bảo đảm an toàn, an ninh mạng, ứng cứu sự cố ATTT mạng, coi nhẹ nhiệm vụ bảo đảm an toàn, an ninh mạng trong công tác quản lý, điều hành dẫn đến một số hệ thống thông tin không đảm bảo an toàn thông tin, có nguy cơ bị xâm nhập, tấn công, mất an toàn hệ thống.

Để tăng cường công tác bảo đảm an toàn, an ninh mạng, tăng cường khả năng phòng, chống các nguy cơ tấn công mạng, bao gồm cả việc ứng cứu sự cố nhằm phục hồi, giảm thiểu thiệt hại, đưa các hệ thống thông tin trở lại hoạt động bình thường trong thời gian sớm nhất khi gặp sự cố tấn công mạng, UBND phường yêu cầu các cơ quan, đơn vị thực hiện nghiêm túc các nội dung sau:

1. Quán triệt nâng cao nhận thức an toàn, an ninh mạng trong toàn hệ thống chính trị và xã hội. Tiếp tục quán triệt thống nhất nhận thức đến từng cán bộ, công chức, viên chức, lực lượng vũ trang chấp hành nghiêm các quy định về đảm bảo an toàn, an ninh

mạng trong hoạt động ứng dụng CNTT, chuyển đổi số. Đẩy mạnh tuyên truyền, vận động các tầng lớp nhân dân nắm rõ tầm quan trọng của việc bảo đảm an toàn, an ninh mạng và vận động người dân cùng chung tay, góp sức thực hiện chuyển đổi số trên địa bàn phường được an toàn, hiệu quả.

2. Nghiêm túc triển khai và thực hiện tốt các quy định của Nhà nước về an toàn thông tin, an ninh mạng, trong đó có các quy định của Luật An toàn thông tin mạng năm 2015; Luật An ninh mạng năm 2018; Luật Bảo vệ bí mật nhà nước năm 2018; Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ về nâng cao năng lực phòng, chống phần mềm độc hại; Chỉ thị số 14/CT-TTg ngày 07/6/2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam; Chỉ thị số 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ về đẩy mạnh triển khai các hoạt động ứng cứu sự cố ATTT mạng Việt Nam và các văn bản chỉ đạo, hướng dẫn của cấp trên về an toàn thông tin, an ninh mạng; Quy định số 85/QĐ/TW ngày 07/10/2022 của Ban Bí thư về việc cán bộ, Đảng viên thiết lập và sử dụng trang thông tin điện tử cá nhân trên internet, mạng xã hội; Quyết định số 874/QĐ-BTTTT ngày 17/6/2021 của Bộ thông tin và truyền thông về ban hành Bộ quy tắc ứng xử trên mạng xã hội.

3. Tăng cường các biện pháp nâng cao an toàn thông tin, an ninh mạng trong toàn hệ thống chính trị của phường.

Các cơ quan, đơn vị xây dựng kế hoạch, phương án đảm bảo an toàn thông tin, an ninh mạng phù hợp và hiệu quả. Đảm bảo việc sử dụng các thiết bị kết nối mạng internet phải được kiểm định đáp ứng các tiêu chuẩn, quy chuẩn kỹ thuật theo quy định; hướng dẫn, đào tạo về an toàn, an ninh mạng cho cán bộ, công nhân viên chức trong đơn vị nắm rõ cách sử dụng.

Bố trí cán bộ phụ trách, bộ phận chuyên trách CNTT của cơ quan, đơn vị thường xuyên phối hợp kiểm tra, rà soát, đánh giá mức độ đảm bảo ATTT cho hệ thống mạng nội bộ (LAN) gồm: Máy chủ, máy trạm, thiết bị mạng, phần cứng, phần mềm hệ thống và các hệ thống thông tin, phần mềm ứng dụng nhằm đánh giá tổng thể mức độ ATTT mạng, kịp thời phát hiện và xử lý sự cố, lỗ hổng, ngăn chặn, bóc gỡ mã độc tấn công vào hệ thống mạng.

Triển khai cài đặt phần mềm chống virus cho tất cả các máy chủ, máy trạm và thiết bị di động trong hệ thống mạng. Sử dụng cơ chế phòng chống tấn công, truy nhập trái phép vào hệ thống mạng, tự động phát hiện và loại trừ mã độc được truyền tải từ thư điện tử, file đính kèm, từ các trang web độc hại trên mạng Internet. Thường xuyên cập nhật

phiên bản mới, bản vá lỗi của hệ điều hành, phần mềm chống virus. Kiểm soát chặt chẽ cài đặt phần mềm trên máy chủ, máy trạm, không cài đặt phần mềm không rõ nguồn gốc hoặc không có bản quyền; cử cán bộ thường xuyên theo dõi hoạt động của cổng/trang thông tin điện tử của đơn vị nhằm tránh các cuộc tấn công deface gây ảnh hưởng đến việc cung cấp thông tin phục vụ người dân và doanh nghiệp. Thiết lập cơ chế bảo mật cho mạng không dây như thay đổi các tham số mặc định của thiết bị, mã hóa dữ liệu, đặt mật khẩu truy cập ở mức an toàn cao nhất.

4. Tăng cường khả năng ứng cứu an toàn, an ninh mạng:

Bộ phận làm nhiệm vụ an toàn, an ninh mạng thực hiện theo đúng chức năng, nhiệm vụ được phân công. Hàng năm phối hợp tổ chức diễn tập thực chiến an toàn thông tin, ứng cứu sự cố khi có yêu cầu nhằm tập huấn, nâng cao năng lực phòng, chống tấn công mạng, đồng thời rút ra bài học kinh nghiệm và phương hướng để đảm bảo an toàn thông tin trên địa bàn phường.

Các phòng, ban, ngành, đoàn thể phối hợp chặt chẽ với Phòng Văn hóa-xã hội, Công an phường để thực hiện giám sát, phòng ngừa và ứng cứu sự cố an toàn thông tin mạng, Cổng/Trang thông tin điện tử tại cơ quan mình.

5. Tăng cường và nâng cao hiệu lực, hiệu quả lãnh đạo, chỉ đạo, quản lý về bảo đảm an toàn, an ninh mạng trên địa bàn.

Quán triệt nguyên tắc trưởng các phòng, ban, ngành, đoàn thể, đơn vị trực tiếp chịu trách nhiệm trước Chủ tịch UBND phường nếu để xảy ra sự cố mất an toàn, an ninh mạng, lộ lọt bí mật Nhà nước trên môi trường mạng tại cơ quan mình.

Triển khai đồng bộ các biện pháp tăng cường đảm bảo thông tin trên môi trường mạng ở mỗi cơ quan, đơn vị trên địa bàn phường.

Mọi tổ chức, cá nhân quản lý chặt chẽ các thiết bị ký số, các tài khoản, mật khẩu được cấp để khai thác hệ thống thông tin, phần mềm nghiệp vụ, đảm bảo tính bảo mật ở mức cao.

Chủ động và tăng cường nắm bắt, dự báo tình hình trong công tác đảm bảo an toàn, an ninh mạng trên địa bàn; tuyên truyền, phổ biến nâng cao nhận thức, hiểu biết và kỹ năng cơ bản bảo đảm an toàn thông tin qua các hệ thống thông tin cơ sở, các phương tiện thông tin đại chúng, truyền thông xã hội.

Triển khai hiệu quả, kịp thời các biện pháp nghiệp vụ để phòng ngừa, phát hiện, đấu tranh, xử lý nghiêm các hành vi xâm phạm an toàn, an ninh thông tin mạng trên địa bàn; thường xuyên phối hợp kiểm tra, đánh giá mức độ đảm bảo an toàn thông tin mạng đối với hệ thống thông tin theo cấp độ phù hợp với quy định của pháp luật.

6. Không tạo, sao chép, lưu trữ cơ sở dữ liệu, tài liệu có chứa thông tin thuộc phạm vi **Bí mật Nhà nước** trên máy tính có kết nối mạng Internet, mạng nội bộ. Kiểm tra an toàn, an ninh thông tin đối với các thiết bị điện tử, giải pháp công nghệ trước khi đưa vào sử dụng tại các bộ phận trọng yếu, cơ mật; loại bỏ triệt để thông tin, tài liệu khi chuyển đổi mục đích sử dụng các thiết bị đã lưu dữ liệu, tài liệu có chứa thông tin thuộc phạm vi bí mật Nhà nước. Kiểm soát việc sửa chữa, thay thế trang thiết bị máy tính trong cơ quan, đơn vị nhằm hạn chế việc lộ lọt, mất thông tin, dữ liệu.

7. Chỉ kết nối đến các hệ thống thông tin, ứng dụng dùng chung của phường tại các cơ quan, đơn vị thông qua mạng truyền số liệu chuyên dùng của phường. Đối với các phần mềm dùng chung, phần mềm chuyên ngành cán bộ, công chức, viên chức, người lao động được cấp tài khoản riêng, yêu cầu thường xuyên thay đổi mật khẩu truy cập. Khi trao đổi thông tin phục vụ công việc Nhà nước, yêu cầu sử dụng hệ thống thư điện tử công vụ dùng chung của phường, của ngành, không sử dụng thư điện tử thương mại, thư điện tử công cộng.

8. Thường xuyên rà soát, thực hiện nâng cấp, chuẩn hóa hạ tầng kỹ thuật CNTT, an toàn, an ninh mạng. Nghiêm túc thực hiện khắc phục kịp thời các lỗ hổng, điểm yếu theo cảnh báo của cơ quan chức năng; chủ động theo dõi, phát hiện sớm các nguy cơ mất an toàn, an ninh mạng để kịp thời xử lý, khắc phục. Có biện pháp kiểm soát nguy cơ mất ATTT mạng gây ra bởi bên thứ ba và các chuỗi cung ứng công nghệ thông tin và truyền thông.

Nhận được công văn này đề nghị các cơ quan, đơn vị tổ chức thực hiện nghiêm túc các nội dung trên, thường xuyên báo cáo tình hình, kết quả thực hiện về UBND phường (qua Công an phường) để theo dõi, hướng dẫn và chỉ đạo./.

Nơi nhận:
- Như trên (để thực hiện);
- Các PCT UBND phường (để p/h chỉ đạo);
- Lưu: VT, CAP.

TM. UỶ BAN NHÂN DÂN
CHỦ TỊCH

Hoàng Nghĩa Thái