

**ỦY BAN NHÂN DÂN
PHƯỜNG PHÙ LIỄN**

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

Số: /UBND-TTHCC
V/v tăng cường công tác bảo đảm an
toàn, an ninh mạng trên địa bàn phường
Phù Liễn

Phù Liễn, ngày tháng năm 2025

Kính gửi:

- Công an phường Phù Liễn;
- Các phòng, trung tâm thuộc phường;
- Các trường học trên địa bàn phường;
- Trung tâm Viễn thông Khu vực 3 - VNPT Hải Phòng.

Ủy ban nhân dân phường Phù Liễn nhận được văn bản số 1803/UBND-NC ngày 07/7/2025 của UBND thành phố về việc tăng cường công tác bảo đảm an toàn, an ninh mạng (*gửi kèm theo*);

Về việc này, UBND phường có ý kiến chỉ đạo như sau:

1. Giao Công an phường Phù Liễn:

- Tham mưu, đề xuất việc đảm bảo an toàn, an ninh mạng, ứng cứu sự cố an toàn thông tin mạng trên địa bàn phường.

- Cử cán bộ đầu mối phụ trách công tác đảm bảo an toàn, an ninh mạng, ứng cứu sự cố an toàn thông tin mạng; thông tin gửi về UBND phường trước ngày 17/7/2025.

- Hướng dẫn các đơn vị triển khai nghiêm túc, hiệu quả công tác bảo đảm an toàn, an ninh mạng, bảo vệ bí mật nhà nước trên không gian mạng trong quá trình sáp nhập, sắp xếp các đơn vị; đẩy mạnh công tác đấu tranh phòng, chống các loại tội phạm mạng, tội phạm sử dụng công nghệ cao lợi dụng việc sắp xếp đơn vị hành chính để thực hiện hành vi vi phạm pháp luật.

2. Đề nghị Trung tâm Viễn thông Khu vực 3 - VNPT Hải Phòng:

Cử cán bộ đầu mối hỗ trợ UBND phường Phù Liễn trong công tác nâng cấp, cải tạo hệ thống đường truyền mạng, hội nghị trực tuyến, dịch vụ công trực tuyến...

3. Yêu cầu các phòng, trung tâm, trường học trên địa bàn phường:

- Tổ chức rà soát toàn bộ hệ thống thông tin trọng yếu, bố trí nhân sự vận hành, thực hiện kết nối, tích hợp, liên thông hệ thống dữ liệu; chủ động xây dựng, triển khai phương án bảo vệ các hệ thống thông tin, cơ sở dữ liệu, tài liệu số và tổ chức bàn giao đúng yêu cầu đối với các đơn vị thuộc diện sắp xếp; tổ chức rà soát, thu hồi các loại USB Token, USB cơ yếu, USB an toàn đối với cán bộ có thay đổi vị trí công tác, hết nhiệm vụ tiếp cận hệ thống dữ liệu, mã hoá; kiểm soát việc phân quyền truy

cập, bảo vệ tài khoản quản trị, tài khoản vận hành hệ thống; chủ động kiểm tra, đánh giá an ninh, an toàn hệ thống mạng, rà quét khắc phục các điểm yếu, lỗ hổng bảo mật; hạ tầng máy chủ, dung lượng truyền tải, các điều kiện cần thiết khác... đảm bảo trước khi kết nối, liên thông hệ thống.

- Đối với các hệ thống thông tin trọng yếu phục vụ trực tiếp công tác lãnh đạo, chỉ đạo của chính quyền địa phương: Hệ thống Quản lý văn bản điện tử, Hệ thống Thư điện tử công vụ, Hệ thống Cổng thông tin điện tử, Hệ thống Tiếp nhận, xử lý dịch vụ công, hệ thống cơ quan phát thanh... yêu cầu các đơn vị thực hiện giám sát 24/7, tăng cường kiểm tra an ninh, an toàn hệ thống, kịp thời phát hiện, khắc phục, ứng cứu sự cố gây mất an ninh, an toàn hệ thống mạng.

Đối với các hệ thống lưu trữ, xử lý thông tin quan trọng, tài liệu bí mật nhà nước chủ động phương án dự phòng hệ thống, sao lưu dữ liệu để bảo đảm khả năng khôi phục khi sự cố xảy ra. Đặc biệt trong giai đoạn chuyển giao công nghệ, đồng bộ dữ liệu trong quá trình sáp nhập, sắp xếp các đơn vị.

- Tăng cường công tác tuyên truyền, phổ biến, hướng dẫn cho người dân trên địa bàn về những thay đổi, điều chỉnh trong thực hiện các dịch vụ công, thủ tục hành chính; cảnh giác trước các phương thức, thủ đoạn hoạt động của các loại tội phạm mạng, tội phạm sử dụng công nghệ cao.

Yêu cầu các đơn vị nghiêm túc triển khai thực hiện./.

Nơi nhận:

- Như trên;
- Lưu: VT, VTHCC.

**TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH**

Phạm Văn Điện