

Số: /KH-UBND

An Dương, ngày tháng năm 2026

KẾ HOẠCH

Triển khai tổng thể các giải pháp giám sát, bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu cho các hệ thống thông tin và hệ thống đường truyền Internet

Thực hiện 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 năm 2026; Kế hoạch số 75/KH-UBND ngày 06/3/2026; Kế hoạch số 76/KH-UBND ngày 06/03/2026 của UBND phường An Dương về việc thực hiện Nghị quyết số 57-NQ/TW, ngày 22/12/2024 của Bộ Chính trị, Ủy ban nhân dân phường xây dựng kế hoạch triển khai tổng thể các giải pháp giám sát, bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu cho các hệ thống thông tin và hệ thống đường truyền Internet như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Nâng cao hiệu quả công tác bảo đảm an toàn thông tin, an ninh mạng đối với các hệ thống thông tin, cơ sở dữ liệu và hạ tầng công nghệ thông tin của UBND phường.
- Chủ động phòng ngừa, phát hiện, cảnh báo và xử lý kịp thời các nguy cơ mất an toàn thông tin, tấn công mạng, rò rỉ hoặc mất dữ liệu.
- Bảo đảm hoạt động ổn định, liên tục của các hệ thống thông tin, hệ thống đường truyền Internet phục vụ công tác chỉ đạo, điều hành, giải quyết thủ tục hành chính và chuyển đổi số.
- Thực hiện các quy định của pháp luật về an ninh mạng, an toàn thông tin mạng và bảo vệ dữ liệu.

2. Yêu cầu

- Triển khai đồng bộ các giải pháp kỹ thuật và quản lý nhằm bảo đảm an toàn thông tin trong phạm vi quản lý.
- Xác định rõ trách nhiệm của từng bộ phận, cán bộ, công chức trong công tác bảo đảm an ninh mạng, bảo mật thông tin và dữ liệu.
- Bảo đảm phù hợp với điều kiện thực tế, tiết kiệm, hiệu quả và đáp ứng yêu cầu chuyển đổi số của địa phương.

II. NỘI DUNG THỰC HIỆN

1. Rà soát, đánh giá hiện trạng hạ tầng công nghệ thông tin

- Kiểm tra, đánh giá hiện trạng hệ thống mạng nội bộ (LAN), hệ thống Wifi, thiết bị mạng, máy chủ, máy tính và các thiết bị đầu cuối.
- Rà soát hiện trạng các hệ thống thông tin, phần mềm dùng chung, cơ sở dữ liệu và hệ thống đường truyền Internet đang khai thác, sử dụng.
- Đánh giá mức độ an toàn của hệ thống đường truyền Internet và mạng nội bộ.
- Xác định các nguy cơ, điểm yếu, lỗ hổng bảo mật và đề xuất phương án khắc phục.

2. Tăng cường giám sát, bảo đảm an ninh mạng

- Thực hiện giám sát thường xuyên hoạt động của hệ thống mạng và các thiết bị công nghệ thông tin.
- Theo dõi, phát hiện sớm các dấu hiệu bất thường, nguy cơ tấn công mạng, mã độc, phần mềm độc hại.
- Phối hợp với cơ quan chuyên môn cấp trên và đơn vị cung cấp dịch vụ để xử lý kịp thời các sự cố phát sinh.

3. Bảo đảm an toàn hệ thống đường truyền Internet

- Chủ động rà soát, nâng cấp đường truyền Internet đáp ứng yêu cầu vận hành các hệ thống thông tin.
- Kiểm tra định kỳ chất lượng đường truyền, bảo đảm kết nối ổn định, liên tục. Duy trì kết nối ổn định, thông suốt với các hệ thống dùng chung của Trung ương và thành phố.
- Xây dựng phương án dự phòng, khắc phục sự cố nhằm hạn chế gián đoạn hoạt động của hệ thống.

4. Bảo mật thông tin và an ninh dữ liệu

- Tăng cường quản lý tài khoản người dùng; thực hiện thay đổi mật khẩu định kỳ và sử dụng mật khẩu có độ an toàn cao.
- Thực hiện sao lưu dữ liệu định kỳ đối với các tài liệu, hồ sơ điện tử và dữ liệu quan trọng.
- Kiểm soát việc chia sẻ, lưu trữ, khai thác dữ liệu; bảo đảm dữ liệu được sử dụng đúng mục đích, đúng thẩm quyền.
- Triển khai các biện pháp bảo vệ dữ liệu cá nhân theo quy định.

5. Cập nhật, nâng cấp hệ thống bảo mật

- Cập nhật thường xuyên hệ điều hành, phần mềm và các bản vá bảo

mật.

- Trang bị, duy trì các giải pháp phòng chống mã độc, tường lửa và các công cụ bảo vệ hệ thống phù hợp với điều kiện thực tế.

- Thực hiện kiểm tra, đánh giá an toàn thông tin định kỳ theo hướng dẫn của cơ quan chuyên môn.

6. Nâng cao nhận thức và năng lực cho cán bộ, công chức

- Tuyên truyền, phổ biến các quy định về an toàn thông tin, an ninh mạng.

- Tổ chức tập huấn, hướng dẫn kỹ năng nhận biết và phòng tránh các nguy cơ mất an toàn thông tin.

- Nâng cao trách nhiệm của cán bộ, công chức trong việc sử dụng hệ thống thông tin và bảo vệ dữ liệu.

III. TỔ CHỨC THỰC HIỆN

1. Văn phòng HĐND và UBND phường

- Là đầu mối tham mưu UBND phường triển khai thực hiện Kế hoạch.

- Thường xuyên kiểm tra, giám sát việc thực hiện các giải pháp bảo đảm an toàn thông tin, an ninh mạng, đôn đốc việc thực hiện của các phòng, đơn vị phường.

- Tổng hợp kết quả thực hiện, báo cáo UBND phường và cơ quan có thẩm quyền theo quy định.

2. Phòng Kinh tế, Hạ tầng và Đô thị

Tham mưu UBND phường bố trí nguồn lực tài chính, ngân sách cho các hoạt động an ninh mạng, các dự án ứng dụng công nghệ thông tin.

3. Phòng Văn hóa - Xã hội

- Thường xuyên tuyên truyền, phổ biến các quy định của pháp luật về an toàn thông tin mạng, bảo vệ dữ liệu cá nhân, bảo mật thông tin trong hoạt động của cơ quan nhà nước đến cán bộ, công chức, viên chức và người lao động.

- Phối hợp với các phòng, đơn vị rà soát, kiểm tra tình trạng hoạt động của hệ thống mạng nội bộ (LAN), hệ thống Internet, các máy tính phục vụ công việc chuyên môn; kịp thời phát hiện và xử lý các nguy cơ mất an toàn thông tin.

- Phối hợp với đơn vị cung cấp dịch vụ viễn thông, công nghệ thông tin duy trì ổn định hệ thống đường truyền Internet phục vụ hoạt động của cơ quan; bảo đảm kết nối thông suốt, an toàn, đáp ứng yêu cầu triển khai chính quyền

số và chuyển đổi số tại địa phương.

- Tham gia các lớp tập huấn, bồi dưỡng kiến thức về an toàn thông tin, an ninh mạng do cấp trên tổ chức; từng bước nâng cao năng lực ứng phó với các sự cố mất an toàn thông tin và tấn công mạng.

4. Trung tâm Dịch vụ sự nghiệp công

Chủ trì công tác tuyên truyền, phổ biến giáo dục pháp luật về bảo đảm an ninh mạng và bảo vệ dữ liệu cá nhân trên Cổng thông tin điện tử, trang facebook, zalo và hệ thống đài truyền thanh và các nền tảng thông tin của địa phương.

5. Công an phường

- Là cơ quan đầu mối, chủ trì thực hiện công tác giám sát, điều phối ứng phó xử lý sự cố an ninh mạng trên địa bàn. Thiết lập kênh tiếp nhận và cam kết thực hiện báo cáo sự cố an ninh mạng trong vòng 24 giờ kể từ khi phát hiện theo quy định.

- Hướng dẫn các phòng, đơn vị rà soát, khắc phục tổng thể về an ninh mạng, bảo mật thông tin đối với hệ thống thông tin và nguồn nhân lực.

IV. CHẾ ĐỘ BÁO CÁO

Các phòng, đơn vị định kỳ 6 tháng, hằng năm hoặc đột xuất báo cáo tình hình thực hiện về Văn phòng HĐND và UBND phường để tổng hợp, tham mưu UBND phường báo cáo cấp có thẩm quyền theo quy định.

Trên đây là Kế hoạch triển khai tổng thể các giải pháp giám sát, bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu cho các hệ thống thông tin và hệ thống đường truyền Internet trong phạm vi quản lý của Ủy ban nhân dân phường An Dương./.

Nơi nhận:

- Chủ tịch, các PCT UBND phường;
- Các phòng, đơn vị thuộc phường;
- Lưu: VT.

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Vũ Mạnh Hùng