UBND THÀNH PHỐ HẢI PHÒNG
SỞ NÔNG NGHIỆP VÀ MÔI TRƯỜNG

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

Số:49 /KH-SNNMT

Hải Phòng, ngày 07 tháng 4 năm 2026

KẾ HOẠCH
Triển khai thi hành Luật An ninh mạng lĩnh vực nông nghiệp và môi trường

Thực hiện Kế hoạch số 97/KH-UBND ngày 26/3/2026 của Ủy ban nhân dân thành phố Triển khai thi hành Luật An ninh mạng trên địa bàn thành phố Hải Phòng;

Sở Nông nghiệp và Môi trường xây dựng Kế hoạch triển khai, cụ thể như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Cụ thể hóa các nhiệm vụ tại Quyết định 437/QĐ-TTg ngày 16/3/2026 của Thủ tướng Chính phủ; Kế hoạch số 97/KH-UBND ngày 26/3/2026 của Ủy ban nhân dân thành phố triển khai thi hành Luật An ninh mạng trên địa bàn thành phố phù hợp với đặc thù ngành nông nghiệp và môi trường.

- Quán triệt đầy đủ các nội dung của Luật An ninh mạng đến toàn thể cán bộ, công chức, viên chức trong ngành nông nghiệp và môi trường.

- Đảm bảo an toàn hệ thống thông tin dữ liệu chuyên ngành.

- Chủ động phòng ngừa, ngăn chặn các nguy cơ tấn công mạng vào hạ tầng thông tin chuyên ngành.

- Đảm bảo an toàn tuyệt đối cho hệ thống dữ liệu dùng chung, dữ liệu chuyên ngành trước các nguy cơ tấn công mạng, gián điệp mạng.

2. Yêu cầu

- 100% cán bộ công chức, viên chức và người lao động nắm vững quy định; 100% hệ thống thông tin quan trọng được phân loại, bảo vệ theo cấp độ.

- Triển khai đồng bộ, có trọng tâm, trọng điểm, không làm gián đoạn các hoạt động chuyên môn, gắn kết chặt chẽ với lộ trình chuyển đổi số của thành phố.

- Nội dung chuyên môn gắn với công tác triển khai thực hiện các nhiệm vụ chính trị và các văn bản có liên quan đến Luật, gắn với trách nhiệm, vai trò của cơ quan chủ trì và các cơ quan phối hợp, các cơ quan, tổ chức có liên quan trong việc triển khai thi hành Luật.

- Xác định rõ trách nhiệm của người đứng đầu, chịu trách nhiệm trực tiếp về an ninh mạng tại đơn vị.

II. NỘI DUNG TRIỂN KHAI

1. Công tác tuyên truyền, tập huấn

- Phổ biến các hành vi bị nghiêm cấm trên không gian mạng; kỹ năng nhận diện thông tin xấu độc liên quan đến chính sách nông nghiệp môi trường và quyền lợi, trách nhiệm của tổ chức, cá nhân.

- Phối hợp với Công an thành phố và Sở Khoa học công nghệ rà soát lỗ hổng mật cho tất cả các website, cổng thông tin thành phần.

- Tuyên truyền, phổ biến các văn bản quy phạm pháp luật, tài liệu hướng dẫn chuyên môn về Luật An ninh mạng; Quyết định số 437/QĐ-TTg ngày 16/3/2026 của Thủ tướng Chính phủ ban hành Kế hoạch triển khai thi hành Luật An ninh mạng.

- Phổ biến văn bản hướng dẫn của Ủy ban nhân dân thành phố, Công an thành phố, Sở Khoa học và Công nghệ về an toàn thông tin mạng, tham gia triển khai các chương trình đào tạo, bồi dưỡng kỹ năng an toàn, an ninh mạng và an toàn thông tin mạng, an ninh thông tin liên quan đến thiết bị camera giám sát.

2. Triển khai phòng ngừa, giám sát phát hiện sự cố mất an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin

- Tổ chức giám sát, phát hiện sớm các nguy cơ, sự cố; kiểm tra, đánh giá an toàn thông tin mạng và rà quét, bóc gỡ, phân tích, xử lý mã độc; phòng ngừa sự cố, quản lý rủi ro; nghiên cứu, phân tích, xác minh, cảnh báo sự cố, rủi ro an toàn thông tin mạng, phần mềm độc hại; xây dựng, áp dụng quy trình, quy định, tiêu chuẩn an toàn thông tin; tuyên truyền, nâng cao nhận thức về nguy cơ, sự cố, tấn công mạng.

- Thực hiện kiểm tra định kỳ và giám sát hệ thống Bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin; an toàn, an ninh thông tin cho thiết bị camera giám sát để phát hiện và ngăn chặn kịp thời các mối đe dọa mạng. Bố trí nguồn lực, kinh phí bảo đảm an toàn thông tin mạng cho các hệ thống thông tin.

3. Hạ tầng đảm bảo an toàn, an ninh thông tin

- Nâng cấp trang thiết bị, công cụ, phương tiện, gia hạn bản quyền phần mềm phục vụ ứng cứu, khắc phục sự cố; chuẩn bị các điều kiện bảo đảm, dự phòng các nguồn lực và tài chính để sẵn sàng đối phó, ứng cứu, khắc phục khi sự cố xảy ra; tổ chức hoạt động của đội ứng cứu sự cố; thuê dịch vụ kỹ thuật và tổ chức, duy trì đội chuyên gia ứng cứu sự cố; tổ chức và tham gia các hoạt động

của mạng lưới ứng cứu sự cố.

- Đảm bảo mạng của hệ thống bảo vệ an toàn bằng cách sử dụng mật khẩu mạnh, cập nhật phần mềm và firmware định kỳ, cài đặt firewall và antivirus.

4. Đánh giá các nguy cơ, sự cố an toàn an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin

- Tổ chức đánh giá hiện trạng và khả năng bảo đảm an toàn thông tin mạng đối với hệ thống thông tin; đánh giá, dự báo các nguy cơ, sự cố tấn công mạng có thể xảy ra với hệ thống thông tin; đánh giá, dự báo các hậu quả, thiệt hại, tác động có thể nếu có xảy ra sự cố; đánh giá về hiện trạng phương tiện, trang thiết bị, công cụ hỗ trợ, nhân lực phục vụ đối phó, ứng cứu, khắc phục sự cố của phòng, đơn vị.

- Thường xuyên đánh giá, kiểm tra nguy cơ tấn công mạng vào hệ thống camera đặc biệt hệ thống camera an ninh không được cập nhật phần mềm định kỳ và các nguy cơ rò rỉ dữ liệu.

5. Xây dựng phương án đối phó, ứng cứu đối với một số tình huống sự cố mất an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin

Đối với mỗi hệ thống thông tin và chương trình ứng dụng, cần xây dựng tình huống, kịch bản sự cố cụ thể và đưa ra phương án đối phó, ứng cứu sự cố tương ứng. Trong phương án đối phó, ứng cứu phải đặt ra được các tiêu chí để có thể nhanh chóng xác định được tính chất, mức độ nghiêm trọng khi sự cố xảy ra. Sở Nông nghiệp và Môi trường xây dựng vận hành hệ thống thông tin, chương trình ứng dụng, xây dựng phương án đối phó, ứng cứu sự cố theo hướng dẫn của Công an thành phố và các đơn vị chuyên môn.

6. Xử lý sự cố, gỡ bỏ và khôi phục

- Xử lý sự cố, gỡ bỏ: Sau khi đã triển khai ngăn chặn sự cố, đơn vị quản lý, vận hành hệ thống thông tin Sở Nông nghiệp và Môi trường phối hợp với Công an thành phố, Sở Khoa học và Công nghệ; Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng thành phố (nếu cần thiết) khẩn trương ngăn chặn sự cố, đồng thời tiêu diệt, gỡ bỏ các mã độc, phần mềm độc hại, khắc phục các điểm yếu an toàn thông tin của hệ thống thông tin.

- Khôi phục: Đơn vị quản lý, vận hành hệ thống thông tin chủ trì phối hợp với các đơn vị liên quan triển khai các hoạt động khôi phục hệ thống thông tin, dữ liệu và kết nối; cấu hình hệ thống an toàn; bổ sung các thiết bị, phần cứng, phần mềm bảo đảm an toàn thông tin của hệ thống thông tin.

II. KINH PHÍ THỰC HIỆN

Kinh phí thực hiện Kế hoạch này được bố trí từ nguồn ngân sách hàng năm của Sở theo quy định của Luật Ngân sách nhà nước và các nguồn kinh phí hợp

pháp khác theo quy định của pháp luật.

III. TỔ CHỨC THỰC HIỆN

1. Văn phòng Sở

- Đầu mối phối hợp với cơ quan chuyên trách (Công an thành phố, Sở Khoa học và Công nghệ), quản lý hệ thống hạ tầng dùng chung, thiết lập quy trình kiểm soát thiết bị lưu trữ ngoài và truy cập từ xa.

- Thực hiện kiểm tra an ninh mạng định kỳ; cài đặt các phần mềm phòng chống mã độc (tại các phòng thuộc khối Văn phòng Sở).

- Xây dựng phương án ứng phó sự cố mạng, thiết lập quy trình phản ứng nhanh khi xảy ra sự cố bị tấn công, chiếm quyền điều khiển hoặc rò rỉ dữ liệu

- Tổ chức diễn tập phòng chống tấn công mạng cho bộ phận chuyên trách công nghệ thông tin của các đơn vị.

- Chủ trì tham mưu, đôn đốc các đơn vị thực hiện; báo cáo định kỳ kết quả triển khai.

- Chủ trì quản trị hệ thống quản lý văn bản, thư công vụ.

- Thực hiện phân quyền truy cập nghiêm ngặt; quản lý đường truyền số liệu chuyên dùng; bố trí kinh phí mua sắm thiết bị bảo mật, phần mềm diệt virus bản quyền cho toàn Sở.

2. Phòng Tài chính Kế hoạch và Đầu tư

- Chủ trì phối hợp với các phòng, đơn vị thực hiện công tác Chuyển đổi số, thực hiện Nghị quyết số 57-NQ/TW ngày 22/12/2024 của Bộ Chính trị gắn với công tác triển khai thi hành Luật An ninh mạng trên địa bàn thành phố.

- Chủ trì tham mưu bố trí kinh phí ngân sách theo lộ trình của Quyết định 437/QĐ-TTg ngày 16/3/2026 của Thủ tướng Chính phủ. Ưu tiên kinh phí cho các giải pháp bảo mật, tham mưu bố trí kinh phí mua sắm thiết bị bảo mật và tổ chức tập huấn.

3. Các phòng, đơn vị trực thuộc Sở

- Ưu tiên sử dụng các thiết bị, giải pháp bảo mật của Việt Nam đã được kiểm định. Triển khai lắp đặt thiết bị bảo mật, cài đặt phần mềm diệt virus tập trung cho toàn bộ máy tính cho đơn vị.

- Chủ động rà soát các hệ thống thông tin, tăng cường giải pháp bảo vệ hệ thống thông tin và bảo đảm thông tin, dữ liệu hoạt động an toàn trên không gian mạng.

- Căn cứ Kế hoạch này có phương án bảo vệ an ninh mạng tại đơn vị mình và thực hiện thi hành Luật An ninh mạng; Quyết định số 437/QĐ-TTg ngày 16/3/2026 của Thủ tướng Chính phủ.

- Trưởng các phòng, Thủ trưởng các đơn vị chịu trách nhiệm về an ninh mạng tại phòng, đơn vị mình phụ trách.

Các phòng, đơn vị gửi báo cáo kết quả triển khai **định kỳ trước ngày 20 của tháng cuối quý** hoặc báo cáo đột xuất khi có yêu cầu về Văn phòng Sở để tổng hợp. Phối hợp với Văn phòng Sở tổ chức thực hiện Kế hoạch này, đảm bảo thực hiện nhiệm vụ an toàn thông tin mạng trong phạm vi quản lý phù hợp với điều kiện thực tế.

Trong quá trình triển khai thực hiện nếu phát sinh khó khăn, vướng mắc, các phòng, đơn vị gửi thông tin về Sở Nông nghiệp và Môi trường (qua Văn phòng Sở) để tổng hợp, điều chỉnh Kế hoạch kịp thời./.

Nơi nhận:
- Giám đốc, các PGĐ Sở;
- Các phòng, đơn vị thuộc Sở;
- Cổng thông tin điện tử Sở;
- Lưu: VT, VP.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HOÀ X.H.C.N VIỆT NAM
SỞ NÔNG NGHIỆP VÀ MÔI TRƯỜNG
THÀNH PHỐ HẢI PHÒNG

Đương Đình Ổn