UBND THÀNH PHỐ HẢI PHÒNG
SỞ NÔNG NGHIỆP VÀ MÔI TRƯỜNG

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

Số: 6492 /SNNMT-VP

Hải Phòng, ngày 05 tháng 6 năm 2026

V/v triển khai công tác bảo đảm an ninh mạng, an ninh thông tin, an ninh dữ liệu

Kính gửi: Các phòng, đơn vị thuộc Sở

Thực hiện ý kiến chỉ đạo của Phó Chủ tịch Ủy ban nhân dân thành phố Hoàng Minh Cường tại Văn bản số 6447/VP-NC ngày 03/6/2026 của Văn phòng Ủy ban nhân dân thành phố *(gửi kèm theo)*;

Giám đốc Sở có ý kiến chỉ đạo các phòng, đơn vị, cụ thể:

1. Tổ chức thực rà soát, đánh giá tổng thể về an ninh mạng, bảo mật thông tin, an ninh dữ liệu, cập nhật, bổ sung chính sách quản lý, quy trình quản trị, giải pháp bảo đảm an ninh mạng cho các hệ thống thông tin tiêu chuẩn quốc gia "TCVN 14423:2025 An ninh mạng - Yêu cầu đối với hệ thống thông tin quan trọng", trong đó ưu tiên rà soát, thực hiện các nội dung:

- **Xác định và phân loại tài sản trong hệ thống thông tin:** Thực hiện rà soát, lập danh mục tất cả tài sản phần cứng, phần mềm, dữ liệu trong hệ thống thông tin. Trong đó, nghiên cứu, đánh giá mức độ quan trọng của từng tài sản làm cơ sở xây dựng và triển khai phương án đảm bảo an ninh mạng cho hệ thống thông tin theo nguyên tắc “bảo vệ đúng, đầu tư đủ”, phân bổ nguồn lực khoa học, tối ưu, tránh gây lãng phí.

- **Xác định và chuẩn hóa mô hình hệ thống thông tin:** Tiến hành rà soát, cập nhật sơ đồ logic và vật lý của hệ thống tin, đảm bảo hệ thống được thiết kế theo nguyên tắc phân chia vùng mạng dựa theo chức năng và tuân thủ nguyên tắc “đặc quyền tối thiểu”, hạn chế tối đa bề mặt tấn công, ngăn chặn rủi ro lây lan khi sự cố xảy ra.

- **Cấu hình bảo mật, rà soát, bóc gỡ mã độc và cập nhật bản vá:** Thực hiện kiểm tra, đánh giá và cấu hình bảo mật toàn bộ các tài sản trong hệ thống thông tin, thứ tự ưu tiên thực hiện dựa theo mức độ quan trọng của tài sản. Khẩn trương cài đặt đầy đủ phần mềm phòng chống mã độc, rà quét, bóc gỡ triệt để mã độc trong hệ thống thông tin, đồng thời cập nhật các bản vá của hệ điều hành, ứng dụng đối với các lỗ hổng bảo mật đã được công bố.

- **Triển khai, kết nối giám sát an ninh mạng:** Thiết lập và duy trì giải pháp giám sát an ninh mạng 24/7 đối với toàn bộ lưu lượng, sự kiện và nhật ký

phần cứng, phần mềm trong hệ thống thông tin, đảm bảo khả năng phát hiện sớm, cảnh báo kịp thời các dấu hiệu bất thường, hành vi xâm nhập trái phép tác động tiêu cực đến hệ thống thông tin. Thực hiện kết nối hệ thống giám sát an ninh mạng về Trung tâm An ninh mạng quốc gia (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an) hoặc Trung tâm An ninh mạng địa phương để chia sẻ thông tin cảnh báo, hỗ trợ giám sát an ninh mạng, kịp thời phát hiện, ngăn chặn các mối đe dọa trên không gian mạng.

- Rà soát, cập nhật quy trình, quy định quản lý, vận hành hệ thống thông tin, đảm bảo an ninh mạng, nâng cao năng lực, trình độ của cán bộ, nhân viên quản trị, vận hành, khai thác hệ thống tin: Tập trung kiện toàn tổ chức, nhân sự và chính sách nội bộ; khẩn trương ban hành các quy chế bảo mật, làm rõ quyền hạn, trách nhiệm của từng cá nhân tham gia quản trị, vận hành, khai thác và bảo vệ hệ thống thông tin. Đồng thời, tổ chức đào tạo nâng cao chuyên môn, nhận thức đảm bảo an ninh mạng cho toàn thể cán bộ, nhân viên nhằm hạn chế rủi ro tấn công mạng, lộ lọt dữ liệu xuất phát từ sự thiếu hiểu biết, thiếu tuân thủ chính sách và tính chủ quan của người dùng.

2. Định kỳ triển khai công tác quản lý rủi ro an ninh mạng nhằm tăng cường khả năng phòng thủ chủ động, thực hiện xác định, đánh giá và triển khai các biện pháp giảm thiểu rủi ro, đồng thời chuẩn bị phương án ứng phó khi rủi ro xảy ra để hạn chế tối đa hậu quả. Chú trọng công tác kiểm tra tuân thủ và cập nhật định kỳ quy định, quy trình hoạt động của bộ phận kỹ thuật, chính sách, quy chế bảo đảm an ninh mạng, quy trình quản trị, vận hành hệ thống, quản lý thay đổi, ứng cứu sự cố; đảm bảo các quy trình, quy định, chính sách được ban hành sát với thực tiễn, có hiệu quả, không mang tính thủ tục, hình thức.

3. Nâng cao hiệu quả công tác bảo đảm an ninh dữ liệu, an ninh thông tin, bảo vệ thông tin thuộc phạm vi bí mật nhà nước thông qua việc tuân thủ tuyệt đối quy định của pháp luật, trong đó tập trung áp dụng các biện pháp cách ly vật lý, mã hóa cơ yếu và kiểm soát chặt chẽ quyền truy cập, tăng cường quản lý định danh, xác thực người dùng ngăn chặn tình trạng thu thập, khai thác và sử dụng trái phép thông tin công dân. Đồng thời, các cơ quan, tổ chức cần triển khai cơ chế quản lý, kiểm soát kỹ thuật đối với toàn bộ vòng đời của dữ liệu, chú trọng các công tác: **(1)** Phân loại, xác định và gắn nhãn mức độ mật, nhạy cảm của tài liệu ngay từ khâu tạo lập, **(2)** Triển khai hệ thống sao lưu dự phòng tách biệt với hệ thống mạng chính, đảm bảo khả năng khục hồi dữ liệu, **(3)** Áp dụng các giải pháp mã hóa đối với dữ liệu trong quá trình lưu trữ và truyền đưa trên môi trường mạng, **(4)** Thực hiện nghiêm quy trình xóa dữ liệu an toàn hoặc tiêu hủy thiết bị lưu trữ khi không còn nhu cầu sử dụng theo quy định.

4. Rà soát, đánh giá khó khăn, vướng mắc việc triển khai, thực hiện Thông báo số 2009/TB-A05-TTANMQG ngày 11/4/2024 của Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an về việc hướng dẫn các biện pháp tăng cường bảo đảm an ninh mạng cho hệ thống thông tin quan trọng về an ninh quốc gia.

Trong quá trình triển khai, thực hiện, nếu gặp khó khăn, vướng mắc, đề nghị đơn vị trao đổi, liên hệ với: Trung tâm An ninh mạng quốc gia - Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an; thư điện tử: contact@nca.gov.vn để được hỗ trợ, đồng thời thông tin về Sở Nông nghiệp và Môi trường (qua Văn phòng Sở) để tổng hợp báo cáo lãnh đạo Sở kịp thời.

Thừa lệnh Giám đốc, Văn phòng Sở thông tin đến các phòng, đơn vị thuộc Sở thực hiện./.

Nơi nhận:
- Như trên;
- GĐ, các PGĐ Sở;
- Lưu: VT, VP.

TL. GIÁM ĐỐC
CHÁNH VĂN PHÒNG

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

Nguyễn Tuấn Ngọc