

Số: 765 /QĐ-BQL

Quảng Ngãi, ngày 30 tháng 9 năm 2026

QUYẾT ĐỊNH

Phê duyệt Phương án Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin đối với Hệ thống thông tin của Ban Quản lý dự án đầu tư xây dựng các công trình Giao thông tỉnh

**GIÁM ĐỐC BAN QUẢN LÝ DỰ ÁN ĐẦU TƯ XÂY DỰNG
CÁC CÔNG TRÌNH GIAO THÔNG TỈNH QUẢNG NGÃI**

*Căn cứ Luật An ninh mạng số 116/2025/QH15 ngày 10/12/2025 của Quốc Hội;
Căn cứ Nghị định số 331/2026/NĐ-CP ngày 19/8/2026 của Chính phủ về bảo vệ an ninh mạng đối với hệ thống thông tin;*

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Căn cứ Quyết định số 2093/QĐ-CAT-ANM ngày 23/9/2026 của Giám đốc Công an tỉnh phê duyệt cấp độ an toàn Hệ thống thông của Ban Quản lý dự án đầu tư xây dựng các công trình Giao thông tỉnh;

Căn cứ Quyết định số 366/QĐ-UBND ngày 01/6/2026 của UBND tỉnh ban hành Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Ban Quản lý dự án đầu tư xây dựng các công trình Giao thông tỉnh;

Theo đề nghị của Chánh Văn phòng.

QUYẾT ĐỊNH:

Điều 1. Phê duyệt Phương án Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin đối với Hệ thống thông tin của Ban Quản lý dự án đầu tư xây dựng các công trình Giao thông tỉnh (có Phương án kèm theo).

Điều 2. Các nội dung trong Phương án là cơ sở để tổ chức thực hiện việc giám sát, theo dõi, phát hiện và cảnh báo các dấu hiệu, nguy cơ mất sự cố an toàn thông tin phát sinh trong quá trình quản lý, vận hành, khai thác Hệ thống thông tin của Ban.

Điều 3. Quyết định này có hiệu lực kể từ ngày ký.

Điều 4. Chánh Văn phòng, Trưởng các phòng chuyên môn nghiệp vụ và toàn thể viên chức, người lao động thuộc Ban chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:

- Như Điều 4;
- Công an tỉnh;
- Lãnh đạo Ban;
- Trưởng các phòng CMNV;
- Trang thông tin điện tử của Ban;
- Lưu: VT, VP.Tâm.

GIÁM ĐỐC


Trần Hoàng Vĩnh

PHƯƠNG ÁN

**Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin đối với
Hệ thống thông tin của Ban Quản lý dự án đầu tư
xây dựng các công trình Giao thông tỉnh**
(Kèm theo Quyết định số 765 /QĐ-BQL ngày 30/9/2026
của Giám đốc Ban Quản lý dự án đầu tư xây dựng
các công trình Giao thông tỉnh)

I. MỤC ĐÍCH

1. Mục đích chung

Thiết lập phương thức thống nhất để giám sát tình trạng hoạt động, phát hiện sớm các dấu hiệu bất thường, nguy cơ mất an toàn thông tin và đưa ra cảnh báo đối với Hệ thống thông tin của Ban Quản lý dự án đầu tư xây dựng các công trình Giao thông tỉnh.

2. Mục tiêu cụ thể

- Theo dõi tình trạng hoạt động và các dấu hiệu bất thường của các thành phần thuộc Hệ thống thông tin trong phạm vi quản lý của Ban.
- Phát hiện sớm các dấu hiệu có khả năng ảnh hưởng đến tính bí mật, toàn vẹn và sẵn sàng của thông tin, dữ liệu và hệ thống.
- Kịp thời ghi nhận, đánh giá và cảnh báo đối với các dấu hiệu bất thường hoặc nguy cơ mất an toàn thông tin.
- Cung cấp thông tin ban đầu, nhật ký và dữ liệu kỹ thuật cần thiết để chuyển sang Phương án Tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng khi xác định có dấu hiệu cần xử lý như một sự cố.
- Hạn chế nguy cơ sự cố phát triển thành sự cố có phạm vi ảnh hưởng lớn.

II. PHẠM VI VÀ ĐỐI TƯỢNG GIÁM SÁT

1. Phạm vi

Phương án áp dụng đối với Hệ thống thông tin, hạ tầng mạng, thiết bị, phần mềm, tài khoản và dữ liệu thuộc phạm vi quản lý, vận hành và sử dụng của Ban.

2. Đối tượng giám sát

Hoạt động giám sát tập trung vào các thành phần sau:

- Hệ thống đường truyền Internet và kết nối mạng;
- Thiết bị tường lửa và các thiết bị bảo vệ mạng;
- Hệ thống mạng LAN, Wi-Fi và các thiết bị chuyển mạch;
- Trang thông tin điện tử Ban;

- Máy tính, máy trạm và thiết bị đầu cuối của người sử dụng;
- Các phần mềm, ứng dụng và hệ thống thông tin được Ban quản lý, khai thác;
- Tài khoản người sử dụng và tài khoản quản trị;
- Dữ liệu và các hệ thống lưu trữ, sao lưu dữ liệu;
- Các thiết bị, hệ thống khác có kết nối vào Hệ thống thông tin của Ban;
- Các nhật ký, cảnh báo an toàn thông tin do thiết bị, phần mềm và hệ thống tạo ra.

III. NGUYÊN TẮC GIÁM SÁT

1. Công tác giám sát được thực hiện thường xuyên, phù hợp với điều kiện thực tế và khả năng kỹ thuật của Ban.
2. Ưu tiên giám sát các thành phần có vai trò quan trọng đối với hoạt động của Hệ thống thông tin, đặc biệt là thiết bị kết nối mạng, tường lửa, thiết bị mạng, máy tính và tài khoản người sử dụng.
3. Việc giám sát phải bảo đảm không làm ảnh hưởng đến hoạt động bình thường của Hệ thống thông tin.
4. Thông tin, nhật ký và dữ liệu thu thập trong quá trình giám sát phải được bảo vệ, tránh truy cập, sửa đổi hoặc xóa trái phép.
5. Khi phát hiện dấu hiệu bất thường, trước hết thực hiện ghi nhận và xác minh cảnh báo; trường hợp xác định có dấu hiệu sự cố thì chuyển thông tin sang Phương án tiếp nhận và xử lý sự cố theo quy định.
6. Phương án này không thay thế quy trình tiếp nhận, phân loại và xử lý sự cố.

IV. QUY TRÌNH GIÁM SÁT, PHÁT HIỆN VÀ CẢNH BÁO

1. Hoạt động giám sát được thực hiện theo quy trình: Thiết bị/hệ thống → Phát sinh nhật ký/cảnh báo → Chuyên viên CNTT → Kiểm tra, xác minh → Phân loại → Cảnh báo/báo cáo → Xử lý → Theo dõi sau xử lý → Lập hồ sơ.
2. Việc giám sát được thực hiện trên cơ sở:
 - Chức năng cảnh báo, ghi nhật ký của thiết bị tường lửa;
 - Nhật ký và trạng thái của thiết bị mạng;
 - Phần mềm phòng, chống mã độc trên máy tính;
 - Nhật ký hệ điều hành, phần mềm và ứng dụng;
 - Thông tin do người sử dụng phản ánh;
 - Cảnh báo từ cơ quan, đơn vị chuyên trách về an toàn thông tin;
 - Cảnh báo, thông tin từ các đơn vị cung cấp dịch vụ, thiết bị, phần mềm.

V. NỘI DUNG GIÁM SÁT

1. Giám sát tình trạng hoạt động của hệ thống

Chuyên viên công nghệ thông tin thực hiện theo dõi:

- Tình trạng hoạt động của kết nối mạng;
- Tình trạng hoạt động của tường lửa;
- Tình trạng hoạt động của các thiết bị mạng;
- Tình trạng hoạt động của máy tính, thiết bị đầu cuối khi có cảnh báo;
- Tình trạng hoạt động của các ứng dụng, phần mềm có liên quan.
- Khi phát hiện thiết bị hoặc thành phần có dấu hiệu hoạt động bất thường, thực hiện ghi nhận để kiểm tra.

2. Giám sát nhật ký

Thực hiện kiểm tra các nguồn nhật ký phù hợp với khả năng kỹ thuật của Ban, bao gồm:

- Nhật ký tường lửa;
- Nhật ký thiết bị mạng;
- Nhật ký hệ điều hành;
- Nhật ký phần mềm bảo vệ;
- Nhật ký đăng nhập;
- Các nhật ký khác có khả năng cung cấp thông tin về dấu hiệu mất an toàn thông tin.
- Việc kiểm tra tập trung vào các dấu hiệu bất thường, không yêu cầu phải phân tích toàn bộ nhật ký theo phương thức chuyên sâu.

3. Giám sát cảnh báo an toàn thông tin

Theo dõi các cảnh báo được tạo ra từ:

- Tường lửa;
- Phần mềm phòng, chống mã độc;
- Hệ điều hành và phần mềm bảo vệ;
- Thiết bị mạng;
- Các hệ thống, phần mềm có chức năng cảnh báo;
- Thông tin cảnh báo từ cơ quan chuyên môn, cơ quan có thẩm quyền.

4. Giám sát dấu hiệu bất thường

Một số dấu hiệu cần chú ý gồm:

- Lưu lượng mạng tăng bất thường;
- Nhiều kết nối bị từ chối trong thời gian ngắn;
- Xuất hiện nhiều lần đăng nhập thất bại;
- Máy tính xuất hiện cảnh báo mã độc;
- Tài khoản có hoạt động bất thường;
- Thiết bị mạng hoạt động không ổn định;

- Xuất hiện thiết bị không xác định trong mạng;
- Dữ liệu hoặc cấu hình có thay đổi bất thường;
- Xuất hiện thư điện tử, liên kết hoặc tệp tin có dấu hiệu nguy hiểm;
- Các dấu hiệu khác do cơ quan chuyên môn cảnh báo.

VI. PHÁT HIỆN VÀ XÁC MINH CẢNH BÁO

1. Tiếp nhận tín hiệu cảnh báo

Khi có cảnh báo từ hệ thống, thiết bị, phần mềm hoặc thông tin do người sử dụng cung cấp, chuyên viên công nghệ thông tin ghi nhận:

- Thời gian phát hiện;
- Nguồn phát hiện;
- Thiết bị hoặc hệ thống liên quan;
- Nội dung cảnh báo;
- Người cung cấp thông tin nếu có;
- Các thông tin kỹ thuật ban đầu.

2. Kiểm tra cảnh báo

Chuyên viên công nghệ thông tin kiểm tra để xác định:

- Cảnh báo có xảy ra thực tế hay không;
- Cảnh báo có phải là cảnh báo nhầm hay không;
- Thành phần nào có liên quan;
- Dấu hiệu bất thường còn tồn tại hay đã kết thúc;
- Có cần tiếp tục theo dõi hay phải chuyển sang quy trình xử lý sự cố.

3. Kết quả xác minh

Sau khi kiểm tra, cảnh báo được xác định theo một trong các trường hợp:

a) Trường hợp 1. Cảnh báo không có dấu hiệu bất thường: Ghi nhận kết quả và kết thúc theo dõi.

b) Trường hợp 2. Cảnh báo chưa đủ cơ sở xác định: Tiếp tục theo dõi, thu thập thêm thông tin và ghi nhận kết quả.

c) Trường hợp 3. Cảnh báo có dấu hiệu nguy cơ: Thực hiện cảnh báo, báo cáo theo quy định và chuyển thông tin cần thiết cho quy trình tiếp nhận, xử lý sự cố khi có đủ căn cứ.

d) Trường hợp 4. Có dấu hiệu sự cố an toàn thông tin: Chuyển ngay thông tin đã xác minh sang Phương án Tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng.

Lưu ý: Phương án này chỉ thực hiện đến bước xác minh và cảnh báo/chuyển thông tin; không thực hiện phân loại mức độ sự cố và xử lý sự cố.

VII. NỘI DUNG VÀ PHƯƠNG THỨC CẢNH BÁO

1. Nội dung cảnh báo

Sau khi tiếp nhận tín hiệu cảnh báo, kiểm tra cảnh báo và xác minh kết quả, chuyên viên công nghệ thông tin cảnh báo đến người sử dụng tối thiểu gồm các nội dung: Thời gian phát hiện; Nội dung cảnh báo; Hệ thống, thiết bị hoặc tài khoản liên quan; Dấu hiệu bất thường; Kết quả kiểm tra ban đầu; Mức độ cần lưu ý của cảnh báo; Kiến nghị tiếp tục theo dõi hoặc chuyển sang quy trình xử lý sự cố.

2. Phương thức cảnh báo

Tùy tính chất thông tin, cảnh báo có thể được thực hiện bằng: Trao đổi trực tiếp; Điện thoại; Thư điện tử công vụ; Hệ thống quản lý, điều hành công việc; Văn bản hoặc hình thức phù hợp khác.

3. Đối tượng nhận cảnh báo

- Văn phòng Ban;
- Các phòng chuyên môn, nghiệp vụ có liên quan;
- Viên chức, người lao động;
- Các đơn vị hỗ trợ kỹ thuật hoặc cơ quan có thẩm quyền khi cần thiết.

VIII. TỔ CHỨC THỰC HIỆN

1. Văn phòng Ban chủ trì tham mưu tổ chức triển khai thực hiện Phương án.
2. Chuyên viên công nghệ thông tin chịu trách nhiệm tham mưu về chuyên môn, kỹ thuật; trực tiếp thực hiện công tác giám sát, phát hiện, xác minh và cảnh báo trong phạm vi được giao.
3. Các phòng chuyên môn nghiệp vụ, viên chức người lao động thuộc Ban có trách nhiệm thực hiện các nội dung của Phương án; chủ động phối hợp và thông báo kịp thời khi phát hiện dấu hiệu mất an toàn thông tin.
4. Phương án này được phổ biến đến toàn thể viên chức, người lao động thuộc Ban biết để thực hiện. Trong quá trình thực hiện nếu có vướng mắc hoặc phát sinh yêu cầu mới, đề nghị các phòng chuyên môn nghiệp vụ, cá nhân kịp thời phản ánh về Văn phòng Ban để tổng hợp báo cáo Giám đốc Ban xem xét, điều chỉnh, bổ sung Phương án cho phù hợp./.