

QUYẾT ĐỊNH

Phê duyệt Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng 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 tin 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 tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng 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 này là căn cứ để tổ chức tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng đối với Hệ thống thông tin của Ban Quản lý dự án đầu tư xây dựng các công trình Giao thông tỉnh và thực hiện các trách nhiệm có liên quan theo quy định.

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;
- Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Công an tỉnh;
- Lãnh đạo Ban;
- Các phòng CMNV;
- Trang thông tin điện tử Ban;
- Lưu: VT, VP.Tâm.



GIÁM ĐỐC

Trần Hoàng Vĩnh

**Tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn
thông tin mạng 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 760/QĐ-BQL ngày 29/9/2026
của Giám đốc Ban Quản lý dự án đầu tư xây dựng
các công trình Giao thông tỉnh)

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- a) Chủ động phát hiện, tiếp nhận và xử lý kịp thời các sự cố mất an toàn thông tin mạng xảy ra đối với Hệ thống thông tin của Ban Quản lý dự án đầu tư xây dựng các công trình Giao thông tỉnh.
- b) Hạn chế thấp nhất nguy cơ mất tính bí mật, toàn vẹn và sẵn sàng của thông tin, dữ liệu thuộc phạm vi quản lý của Ban.
- c) Xác định rõ trách nhiệm của từng cá nhân, bộ phận trong việc phát hiện, thông báo, tiếp nhận, xác minh, phân loại và xử lý ban đầu sự cố.
- d) Bảo đảm khi xảy ra sự cố vượt quá khả năng xử lý của Ban thì được báo cáo, phối hợp và đề nghị cơ quan chuyên trách, đơn vị cung cấp dịch vụ hoặc cơ quan có thẩm quyền hỗ trợ kịp thời.

2. Yêu cầu

- a) Việc xử lý sự cố phải được thực hiện nhanh chóng, đúng thẩm quyền, có kiểm soát và hạn chế tối đa việc làm mất hoặc thay đổi chứng cứ liên quan đến sự cố.
- b) Không tự ý xóa dữ liệu, nhật ký, bằng chứng hoặc cài đặt lại hệ thống khi chưa đánh giá ảnh hưởng và chưa thực hiện các biện pháp cần thiết để bảo toàn thông tin phục vụ xác minh sự cố.
- c) Mọi sự cố phải được ghi nhận, theo dõi và lưu hồ sơ.
- d) Các sự cố có dấu hiệu nghiêm trọng hoặc vượt khả năng xử lý phải được báo cáo ngay lãnh đạo Ban và phối hợp với cơ quan, đơn vị chuyên trách về an toàn thông tin (ATTT) theo quy định.

II. PHẠM VI VÀ ĐỐI TƯỢNG ÁP DỤNG

1. Phạm vi

Phương án này áp dụng đối với Hệ thống thông tin của Ban Quản lý dự án đầu tư xây dựng các công trình Giao thông tỉnh và các thành phần có liên quan, bao gồm:

- Hệ thống mạng LAN, Internet, Wi-Fi;
- Thiết bị tường lửa, thiết bị mạng, thiết bị định tuyến/chuyển mạch;
- Máy tính, máy trạm của viên chức, người lao động;
- Hệ thống thư điện tử và các hệ thống phần mềm dùng chung;
- Trang thông tin điện tử của Ban;

- Các hệ thống, phần mềm phục vụ công tác quản lý, điều hành;
- Hệ thống camera giám sát, thiết bị kết nối mạng thuộc phạm vi quản lý;
- Dữ liệu điện tử, tài khoản người dùng, tài khoản quản trị;
- Các dịch vụ CNTT do đơn vị cung cấp dịch vụ, doanh nghiệp viễn thông hoặc nhà cung cấp khác thực hiện.

2. Đối tượng áp dụng

- Viên chức và người lao động thuộc Ban.
- Các đơn vị cung cấp dịch vụ CNTT, viễn thông, bảo mật và các đơn vị liên quan.

III. NGUYÊN TẮC XỬ LÝ SỰ CỐ

1. Phát hiện sớm - thông báo nhanh - xử lý đúng thẩm quyền.

2. Ưu tiên bảo vệ:

- Con người và hoạt động của Ban;
- Tính sẵn sàng của hệ thống;
- Tính toàn vẹn của dữ liệu;
- Tính bí mật của thông tin.

3. Không tự ý thực hiện các thao tác có khả năng làm mất dấu vết hoặc chứng cứ của sự cố.

4. Sự cố phải được phân loại sơ bộ ngay sau khi xác minh.

5. Đối với sự cố vượt khả năng xử lý của Ban, phải kịp thời đề nghị hỗ trợ.

6. Việc ứng cứu sự cố thực hiện theo quy định của pháp luật và phương án ứng cứu sự cố đã được cấp có thẩm quyền phê duyệt. Khi phát hiện hoặc tiếp nhận sự cố phải ghi nhận, tập hợp thông tin, phản hồi việc tiếp nhận, xác minh, đánh giá và triển khai xử lý ban đầu; nếu có khả năng là sự cố nghiêm trọng thì phải báo cáo để xem xét nâng cấp sự cố.

IV. TỔ CHỨC TIẾP NHẬN VÀ PHÁT HIỆN SỰ CỐ

1. Các nguồn phát hiện sự cố

Sự cố có thể được phát hiện từ:

a) Người sử dụng

- Viên chức, người lao động phát hiện;
- Máy tính hoạt động bất thường;
- Không đăng nhập được tài khoản;
- Xuất hiện tệp tin hoặc chương trình bất thường;
- Có dấu hiệu mã độc;
- Tài khoản bị sử dụng trái phép;
- Nhận được thư điện tử đáng ngờ;
- Dữ liệu bị thay đổi, mất hoặc không thể truy cập;
- Trang thông tin điện tử có biểu hiện bất thường.

b) Chuyên viên CNTT

- Kiểm tra hệ thống mạng;

- Kiểm tra thiết bị tường lửa;
- Kiểm tra máy trạm;
- Kiểm tra nhật ký hệ thống;
- Theo dõi cảnh báo bảo mật;
- Theo dõi tình ứng dụng và dịch vụ;
- Tiếp nhận phản ánh của người sử dụng.

c) Nhà cung cấp dịch vụ

Nhà cung cấp đường truyền Internet, thiết bị bảo mật, phần mềm hoặc dịch vụ CNTT phát hiện nguy cơ, tấn công hoặc sự cố phải thông báo cho chuyên viên CNTT.

d) Cơ quan chuyên trách về ATTT

Ban sẽ tiếp nhận cảnh báo, thông báo về nguy cơ hoặc sự cố từ cơ quan chuyên trách về ATTT, cơ quan điều phối hoặc các cơ quan có thẩm quyền.

V. ĐẦU MỐI TIẾP NHẬN SỰ CỐ

1. Đầu mối chính

- Văn phòng Ban là đầu mối tiếp nhận và tham mưu xử lý sự cố ATTT của Ban.
- Chuyên viên CNTT là đầu mối kỹ thuật trực tiếp tiếp nhận, kiểm tra, xác minh và xử lý ban đầu.

2. Kênh tiếp nhận

Có thể tiếp nhận sự cố thông qua: Trực tiếp; điện thoại; Email công vụ; hệ thống quản lý văn bản; nhóm trao đổi công việc nội bộ; văn bản hoặc thông báo của các phòng chuyên môn nghiệp vụ (CMNV).

3. Thông tin tối thiểu khi thông báo

Thời điểm phát hiện; thiết bị/hệ thống xảy ra sự cố; biểu hiện bất thường; tình trạng hiện tại; ảnh chụp màn hình nếu có; các thao tác đã thực hiện trước khi xảy ra sự cố; thông tin khác có liên quan.

VI. QUY TRÌNH TIẾP NHẬN VÀ PHÁT HIỆN SỰ CỐ

Quy trình thực hiện theo 06 bước:

- Bước 1. Phát hiện sự cố: Người sử dụng hoặc hệ thống kỹ thuật phát hiện dấu hiệu bất thường.
- Bước 2. Thông báo: Người sử dụng thông báo ngay cho Văn phòng hoặc chuyên viên CNTT.
- Bước 3. Ghi nhận: Chuyên viên CNTT ghi nhận thời gian; người thông báo; thiết bị/hệ thống; biểu hiện; phạm vi ảnh hưởng sơ bộ.
- Bước 4. Xác minh: Kiểm tra hệ thống, thiết bị, nhật ký, tài khoản, kết nối mạng và các thông tin liên quan.
- Bước 5. Phân loại: Xác định sự cố thông thường, nghiêm trọng hoặc vượt khả năng xử lý.
- Bước 6. Xử lý ban đầu: Áp dụng biện pháp cô lập, ngăn chặn, khôi phục hoặc đề nghị hỗ trợ phù hợp.

VII. QUY TRÌNH XỬ LÝ BAN ĐẦU

Quy trình thực hiện 07 bước đối với Chuyên viên CNTT

- Bước 1: Tiếp nhận thông tin sự cố vào Phiếu ghi nhận sự cố ATTT.
- Bước 2: Xác định có phải sự cố ATTT hay không; hệ thống/thiết bị bị ảnh hưởng; thời gian xảy ra; nguyên nhân sơ bộ; phạm vi ảnh hưởng.
- Bước 3: Cô lập ngắt kết nối thiết bị; chặn tài khoản; chặn địa chỉ kết nối; tạm dừng dịch vụ bị ảnh hưởng; cô lập vùng mạng liên quan.
- Bước 4: Ngăn chặn áp dụng các biện pháp phù hợp để hạn chế sự cố lan rộng.
- Bước 5: Khắc phục ban đầu trong khả năng như khôi phục kết nối; xử lý mã độc; khôi phục tài khoản; khôi phục dịch vụ; khôi phục dữ liệu từ bản sao lưu; điều chỉnh cấu hình an toàn.
- Bước 6: Báo cáo nếu trường hợp sự cố vượt khả năng xử lý hoặc có dấu hiệu nghiêm trọng, Chuyên viên CNTT báo cáo Văn phòng Ban đề tham mưu Giám đốc chỉ đạo và đề nghị cơ quan chuyên trách/đơn vị liên quan hỗ trợ.
- Bước 7: Sau khi hệ thống ổn định phải Ghi nhận kết quả; lưu hồ sơ; xác định nguyên nhân; đề xuất biện pháp phòng ngừa tái diễn.

VIII. TRÁCH NHIỆM CỦA CÁC BỘ PHẬN, CÁ NHÂN

1. Giám đốc Ban

Chỉ đạo chung trong công tác xử lý sự cố; quyết định huy động nguồn lực khi cần thiết; chỉ đạo báo cáo cơ quan có thẩm quyền; chỉ đạo phối hợp với cơ quan chuyên trách, đơn vị cung cấp dịch vụ; chỉ đạo khắc phục và phòng ngừa tái diễn.

2. Văn phòng

Là đầu mối tổ chức tiếp nhận và điều phối xử lý sự cố; tiếp nhận báo cáo từ Chuyên viên CNTT; tham mưu Giám đốc chỉ đạo xử lý; phối hợp các phòng CMNV theo dõi quá trình xử lý; lưu hồ sơ, báo cáo sự cố.

3. Chuyên viên CNTT:

Là đầu mối kỹ thuật: Theo dõi, kiểm tra và phát hiện sự cố; tiếp nhận phản ánh; xác minh sự cố; phân loại sơ bộ; thực hiện xử lý ban đầu; kiểm tra nhật ký; bảo toàn thông tin, dữ liệu liên quan; phối hợp nhà cung cấp; báo cáo Văn phòng Ban tham mưu đề xuất Giám đốc huy động chuyên gia hoặc cơ quan chuyên trách khi vượt khả năng xử lý.

4. Người sử dụng

Viên chức, người lao động có trách nhiệm: Bảo vệ tài khoản; mail công vụ, không chia sẻ mật khẩu; không tự ý cài đặt phần mềm không được phép; thông báo ngay sự cố; không tự ý xóa dữ liệu hoặc xử lý sự cố khi chưa được hướng dẫn.

5. Đơn vị cung cấp dịch vụ

Tiếp nhận yêu cầu hỗ trợ; phối hợp xác minh nguyên nhân; thực hiện xử lý theo phạm vi trách nhiệm; cung cấp thông tin nhật ký, cảnh báo hoặc thông tin kỹ thuật liên quan; hỗ trợ khôi phục hoạt động bình thường.

IX. CHẾ ĐỘ GHI NHẬN VÀ BÁO CÁO

Mỗi sự cố phải được lập hồ sơ tối thiểu gồm:

1. Phiếu tiếp nhận sự cố;
2. Thông tin người phát hiện;
3. Thời gian phát hiện;
4. Mô tả sự cố;
5. Thiết bị/hệ thống bị ảnh hưởng;
6. Kết quả xác minh;
7. Phân loại sự cố;
8. Biện pháp xử lý ban đầu;
9. Kết quả xử lý;
10. Đơn vị/cá nhân phối hợp;
11. Kiến nghị, đề xuất;
12. Tài liệu, hình ảnh, nhật ký hoặc thông tin liên quan.

X. TỔ CHỨC THỰC HIỆN

1. Văn phòng Ban

- Văn phòng Ban chủ trì, tham mưu Giám đốc Ban tổ chức triển khai thực hiện Phương án.

- Theo dõi, đôn đốc việc thực hiện các quy trình xử lý sự cố; tổng hợp tình hình, kết quả thực hiện và tham mưu Giám đốc Ban chỉ đạo xử lý khi phát sinh sự cố an toàn thông tin, an ninh mạng.

- Làm đầu mối phối hợp với các cơ quan, đơn vị có liên quan trong trường hợp sự cố vượt quá khả năng xử lý của Ban hoặc cần sự hỗ trợ về chuyên môn, kỹ thuật.

2. Chuyên viên CNTT

- Chuyên viên CNTT chịu trách nhiệm tham mưu về chuyên môn, kỹ thuật trong việc triển khai và thực hiện Phương án; theo dõi, giám sát tình trạng hoạt động của hệ thống thông tin, mạng nội bộ, thiết bị và các giải pháp bảo đảm an toàn thông tin thuộc phạm vi quản lý của Ban.

- Thực hiện rà soát, cập nhật các nguy cơ, rủi ro và phương thức xử lý sự cố; tham gia tiếp nhận, phân tích, xử lý, khắc phục và phối hợp ứng phó khi xảy ra sự cố an toàn thông tin, an ninh mạng.

- Định kỳ hoặc khi có yêu cầu, tham mưu Văn phòng Ban báo cáo Giám đốc Ban về tình hình an toàn thông tin và đề xuất các biện pháp xử lý, khắc phục, phòng ngừa sự cố.

- Chủ động rà soát, đề xuất cập nhật, điều chỉnh Phương án để phù hợp với hiện trạng hệ thống thông tin, hạ tầng kỹ thuật, yêu cầu bảo đảm an toàn thông tin và các quy định có liên quan.

3. Trưởng các phòng CMNV

- Trưởng các phòng CMNV có trách nhiệm phổ biến cho viên chức, người lao động của phòng tổ chức thực hiện các nội dung của Phương án; quán triệt việc quản lý, sử dụng hệ thống thông tin, máy tính, thiết bị và tài khoản được giao đúng quy định.

- Chủ động phát hiện, kịp thời thông báo cho Văn phòng Ban hoặc chuyên viên CNTT khi phát hiện dấu hiệu bất thường, nguy cơ mất an toàn thông tin hoặc xảy ra sự cố liên quan đến hệ thống, thiết bị, tài khoản và dữ liệu thuộc phạm vi quản lý, sử dụng.

- Phối hợp cung cấp thông tin, hiện trạng và thực hiện các yêu cầu cần thiết để phục vụ việc xác định nguyên nhân, xử lý, khắc phục và phòng ngừa tái diễn sự cố.

4. Viên chức, người lao động

- Viên chức, người lao động có trách nhiệm tuân thủ các quy định về bảo đảm an toàn thông tin; bảo vệ tài khoản, mật khẩu và các thông tin xác thực được giao; không tự ý chia sẻ tài khoản, mật khẩu hoặc cho người khác sử dụng tài khoản của mình.

- Không tự ý cài đặt phần mềm, thay đổi cấu hình thiết bị hoặc thực hiện các thao tác có nguy cơ ảnh hưởng đến an toàn, bảo mật của hệ thống.

- Khi phát hiện sự cố hoặc dấu hiệu nghi ngờ mất an toàn thông tin, phải kịp thời thông báo cho Văn phòng Ban hoặc chuyên viên CNTT để được hướng dẫn, xử lý; không tự ý xóa, sửa hoặc làm thay đổi dữ liệu, nhật ký và các thông tin có liên quan đến sự cố.

5. Rà soát, cập nhật Phương án

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 và cần sửa đổi, bổ sung, đề nghị các phòng CMNV, cá nhân kịp thời phản ánh về Văn phòng Ban để tổng hợp báo cáo Giám đốc Ban xem xét, sửa đổi, bổ sung cho phù hợp./.
