

KẾ HOẠCH

Triển khai công tác bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu tại Ban Quản lý dự án đầu tư xây dựng các công trình Giao thông tỉnh Quảng Ngãi năm 2026

Căn cứ Kế hoạch số 02-KH/BCĐ ngày 24/4/2026 của Ban Chỉ đạo về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số tỉnh về bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong hệ thống chính trị trên địa bàn tỉnh Quảng Ngãi;

Căn cứ Công văn số 4447/UBND-KGVX ngày 18/5/2026 của UBND tỉnh về việc bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong hệ thống chính trị trên địa bàn tỉnh Quảng Ngãi;

Ban Quản lý dự án đầu tư xây dựng các công trình Giao thông tỉnh (*viết tắt là Ban QLDA*) ban hành Kế hoạch triển khai công tác bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu năm 2026, cụ thể như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

a) Tổ chức triển khai đầy đủ, thiết thực các nhiệm vụ về bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu theo Kế hoạch số 02-KH/BCĐ ngày 24/4/2026 và chỉ đạo của UBND tỉnh, phù hợp với chức năng, nhiệm vụ và điều kiện thực tế của Ban.

b) Chủ động phòng ngừa, phát hiện, xử lý và khắc phục các nguy cơ, lỗ hổng, sự cố mất an toàn thông tin đối với hệ thống thông tin, mạng máy tính, thiết bị công nghệ thông tin, tài khoản người dùng và dữ liệu do Ban quản lý, khai thác và sử dụng.

c) Nâng cao trách nhiệm của người đứng đầu, các phòng chuyên môn nghiệp vụ (*viết tắt là CMNV*), viên chức, người lao động trong việc bảo vệ hệ thống thông tin, bảo mật thông tin và bảo đảm an toàn dữ liệu trong quá trình thực hiện nhiệm vụ.

d) Từng bước hình thành phương thức quản lý an toàn thông tin theo hướng chủ động phòng ngừa, quản lý rủi ro và ứng phó kịp thời khi xảy ra sự cố.

2. Yêu cầu

a) Công tác bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu phải được thực hiện thường xuyên, liên tục, gắn với hoạt động quản lý, điều hành và thực hiện nhiệm vụ chuyên môn của Ban.

b) Xác định rõ trách nhiệm của người đứng đầu, chuyên viên công nghệ thông tin, các phòng CMNV, từng cá nhân trong việc quản lý, sử dụng và bảo vệ hệ thống thông tin, tài khoản, dữ liệu.

c) Ưu tiên các giải pháp thiết thực, phù hợp với hiện trạng hạ tầng công nghệ thông tin và khả năng nguồn lực của Ban; tránh đầu tư dàn trải, không hiệu quả.

II. MỤC TIÊU

1. Mục tiêu chung

Bảo đảm hệ thống thông tin, hạ tầng mạng, thiết bị công nghệ thông tin và dữ liệu phục vụ công tác quản lý, điều hành và quản lý dự án của Ban hoạt động an toàn, ổn định; hạn chế nguy cơ mất an toàn thông tin, rò rỉ dữ liệu, mã độc và các hành vi truy cập trái phép.

2. Mục tiêu cụ thể năm 2026

a) 100% hệ thống thông tin, thiết bị hạ tầng mạng và các thiết bị công nghệ thông tin quan trọng thuộc phạm vi quản lý của Ban được rà soát, đánh giá hiện trạng và xác định nguy cơ mất an toàn thông tin.

b) 100% tài khoản mail công vụ, phần mềm ký số của Ban được rà soát về người sử dụng, quyền truy cập và tình trạng hoạt động.

c) 100% viên chức, người lao động được tuyên truyền, phổ biến các quy định và kỹ năng cơ bản về bảo đảm an toàn thông tin.

d) Hoàn thiện, cập nhật hồ sơ đề xuất cấp độ an toàn hệ thống thông tin của Ban theo quy định và phối hợp với cơ quan có thẩm quyền trong quá trình thẩm định, phê duyệt, kiểm tra khi có yêu cầu.

đ) Các lỗ hổng, điểm yếu có nguy cơ cao được xử lý, khắc phục hoặc có biện pháp kiểm soát rủi ro phù hợp.

e) Dữ liệu quan trọng phục vụ hoạt động quản lý, điều hành và quản lý dự án có phương án sao lưu phù hợp.

g) Duy trì lực lượng Đội ứng cứu sự cố thông tin của Ban; bảo đảm khi phát sinh sự cố có đầu mối tiếp nhận, xử lý, báo cáo và phối hợp với cơ quan chuyên trách.

III. PHẠM VI THỰC HIỆN

1. Hệ thống mạng nội bộ, mạng không dây, thiết bị bảo vệ mạng, thiết bị chuyển mạch, thiết bị kết nối Internet, hệ thống camera và các thiết bị công nghệ thông tin khác thuộc phạm vi quản lý của Ban.

2. Máy tính, thiết bị đầu cuối, thiết bị lưu trữ và các thiết bị có kết nối vào hệ thống mạng của Ban.

3. Các hệ thống, phần mềm, tài khoản và dịch vụ số phục vụ công tác quản lý, điều hành và chuyên môn của Ban, bao gồm hệ thống quản lý văn bản và điều

hành, thư điện tử, chữ ký số, SIM PKI, Trang thông tin điện tử, các phần mềm nghiệp vụ và các dịch vụ số khác đang được sử dụng.

4. Dữ liệu, hồ sơ điện tử, tài liệu công việc, dữ liệu quản lý dự án và các thông tin khác được tạo lập, lưu trữ, trao đổi và khai thác trong quá trình thực hiện nhiệm vụ.

IV. NHIỆM VỤ VÀ GIẢI PHÁP

1. Tăng cường trách nhiệm của người đứng đầu

a) Giám đốc Ban trực tiếp chỉ đạo công tác bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu; xem xét, quyết định các biện pháp cần thiết để bảo đảm an toàn cho hệ thống thông tin và dữ liệu của Ban.

b) Các Phó Giám đốc Ban theo lĩnh vực, dự án được phân công có trách nhiệm chỉ đạo các phòng CMNV thuộc phạm vi phụ trách thực hiện nghiêm các quy định về bảo đảm an toàn thông tin, bảo mật dữ liệu trong quá trình thực hiện nhiệm vụ.

c) Trưởng các phòng CMNV chịu trách nhiệm quán triệt viên chức, người lao động thuộc phạm vi quản lý; chủ động phát hiện và thông báo kịp thời về Văn phòng Ban qua chuyên viên công nghệ thông tin khi có dấu hiệu bất thường hoặc nguy cơ mất an toàn thông tin.

2. Rà soát, kiểm kê và đánh giá hệ thống thông tin

a) Rà soát, cập nhật danh mục hệ thống thông tin, phần mềm, thiết bị mạng, thiết bị đầu cuối và các tài sản công nghệ thông tin đang được sử dụng tại Ban.

b) Xác định hệ thống, thiết bị, phần mềm và dữ liệu quan trọng cần ưu tiên bảo vệ.

c) Rà soát sơ đồ kết nối mạng, cấu hình thiết bị mạng và thiết bị bảo vệ; kiểm tra việc phân tách, kiểm soát truy cập giữa các thành phần mạng phù hợp với điều kiện thực tế.

d) Kiểm tra tình trạng hoạt động, cập nhật phần mềm, hệ điều hành, phần mềm phòng chống mã độc và các giải pháp bảo vệ đang sử dụng.

đ) Lập danh sách các điểm yếu, nguy cơ, lỗ hổng phát hiện trong quá trình rà soát và đề xuất phương án xử lý.

3. Bảo đảm an toàn hệ thống thông tin theo cấp độ

a) Xây dựng các phương án quản lý sự cố an toàn thông tin mạng theo hồ sơ cấp độ 2.

b) Phối hợp với Công an tỉnh và các cơ quan chuyên môn có liên quan trong việc thẩm định, phê duyệt, kiểm tra, hướng dẫn và xử lý các vấn đề về an toàn hệ thống thông tin theo thẩm quyền.

c) Khi có yêu cầu kết nối, chia sẻ dữ liệu giám sát an toàn thông tin tập trung của tỉnh hoặc cơ quan chuyên trách, Ban thực hiện phối hợp, cung cấp thông tin và tổ chức kết nối theo hướng dẫn của cơ quan có thẩm quyền.

4. Bảo vệ dữ liệu và thông tin

a) Rà soát, phân loại dữ liệu phục vụ hoạt động của Ban theo mức độ cần bảo vệ, trong đó chú trọng dữ liệu quản lý dự án, hồ sơ thiết kế, hồ sơ đấu thầu, hợp đồng, tài liệu tài chính, dữ liệu nhân sự, tài khoản và các thông tin nội bộ khác.

b) Xác định người chịu trách nhiệm quản lý đối với từng nhóm dữ liệu; hạn chế việc truy cập, sao chép, tải xuống hoặc chia sẻ dữ liệu không đúng thẩm quyền.

c) Khi gửi, nhận hoặc chia sẻ tài liệu điện tử phải kiểm tra đúng người nhận, đúng phạm vi và đúng mục đích công việc; đối với dữ liệu quan trọng, thực hiện sao lưu định kỳ và kiểm tra khả năng phục hồi dữ liệu.

5. Quản lý tài khoản và phân quyền truy cập

a) Rà soát toàn bộ tài khoản đang sử dụng trên các hệ thống, phần mềm; kịp thời vô hiệu hóa các tài khoản mail công vụ đã chuyển công tác hoặc thôi việc.

b) Việc cấp, thay đổi, thu hồi quyền truy cập phải gắn với vị trí, nhiệm vụ và phạm vi công việc của người sử dụng.

c) Không sử dụng chung tài khoản cá nhân; không cung cấp mật khẩu, mã xác thực hoặc thông tin bảo mật cho người khác.

6. Bảo đảm an toàn thiết bị đầu cuối

a) Thực hiện cập nhật hệ điều hành, phần mềm và bản vá bảo mật phù hợp.

b) Duy trì phần mềm phòng chống mã độc và thực hiện kiểm tra định kỳ đối với máy tính, thiết bị đầu cuối.

c) Không tự ý cài đặt phần mềm không rõ nguồn gốc, phần mềm không được phép hoặc phần mềm có nguy cơ ảnh hưởng đến an toàn hệ thống.

d) Hạn chế sử dụng thiết bị lưu trữ di động không rõ nguồn gốc; kiểm tra thiết bị trước khi sử dụng.

đ) Khi phát hiện máy tính có dấu hiệu bất thường như xuất hiện cảnh báo mã độc, tự động mở trang web, mất dữ liệu, hoạt động bất thường hoặc không truy cập được hệ thống, người sử dụng phải báo ngay cho chuyên viên công nghệ thông tin.

7. Bảo đảm an toàn hạ tầng mạng

a) Kiểm tra, rà soát cấu hình thiết bị bảo vệ mạng, thiết bị cân bằng tải, thiết bị tường lửa, thiết bị chuyển mạch, mạng không dây và các thiết bị liên quan.

b) Rà soát việc sử dụng mạng không dây; thay đổi mật khẩu khi cần thiết và hạn chế chia sẻ thông tin truy cập cho người không có nhiệm vụ.

c) Rà soát hệ thống camera và các thiết bị có kết nối mạng nhằm hạn chế nguy cơ bị truy cập trái phép hoặc sử dụng làm điểm trung gian tấn công vào hệ thống.

8. Sao lưu, phục hồi và bảo vệ dữ liệu

a) Thực hiện sao lưu định kỳ đối với các dữ liệu quan trọng phục vụ công tác quản lý, điều hành và quản lý dự án.

b) Kiểm tra định kỳ các bản sao lưu để đảm bảo phục hồi dữ liệu khi cần thiết.

c) Bảo đảm bản sao lưu được quản lý, bảo vệ và hạn chế quyền truy cập trái phép.

9. Rà soát, phát hiện và xử lý lỗ hổng

a) Thường xuyên theo dõi các cảnh báo về lỗ hổng, mã độc và nguy cơ mất an toàn thông tin từ cơ quan chuyên trách, đơn vị cung cấp dịch vụ và các nguồn cảnh báo chính thống.

b) Ưu tiên xử lý các lỗ hổng có mức độ nghiêm trọng cao, các lỗ hổng ảnh hưởng trực tiếp đến hệ thống kết nối Internet, thiết bị bảo vệ mạng, phần mềm và dữ liệu quan trọng.

c) Lưu hồ sơ theo dõi việc phát hiện, xử lý và khắc phục lỗ hổng để phục vụ kiểm tra, đánh giá.

10. Phòng ngừa và ứng cứu sự cố

a) Duy trì Đội ứng cứu sự cố an toàn thông tin của Ban, bảo đảm có đầu mối tiếp nhận và xử lý sự cố.

b) Các sự cố có nguy cơ ảnh hưởng đến hệ thống, dữ liệu hoặc hoạt động của Ban phải được ghi nhận, đánh giá, xử lý và báo cáo theo quy định.

c) Không tự ý xóa dữ liệu, cài đặt lại máy tính hoặc thay đổi hiện trạng thiết bị khi đang xảy ra sự cố nghiêm trọng nếu việc này có thể làm mất dấu vết phục vụ xác định nguyên nhân.

11. Nâng cao nhận thức, kỹ năng an toàn thông tin

a) Tổ chức phổ biến cho toàn thể viên chức, người lao động các nội dung cơ bản về:

- Nhận diện thư điện tử, đường link, tệp tin có dấu hiệu lừa đảo;
- Bảo vệ mật khẩu và tài khoản;
- Sử dụng chữ ký số, tài khoản hệ thống;
- Phòng chống mã độc;
- Bảo vệ dữ liệu và tài liệu công việc;
- Xử lý khi phát hiện sự cố an toàn thông tin.

b) Lồng ghép nội dung an toàn thông tin trong các cuộc họp, sinh hoạt chuyên môn, tập huấn, hướng dẫn sử dụng phần mềm và các hoạt động chuyển đổi số của Ban.

V. TRÁCH NHIỆM

1. Giám đốc Ban QLDA

Chịu trách nhiệm chung về công tác bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu tại Ban; chỉ đạo triển khai Kế hoạch; phê duyệt các nội dung, phương án xử lý thuộc thẩm quyền; chỉ đạo huy động nguồn lực và xử lý các vấn

đề phát sinh, đặc biệt đối với sự cố có nguy cơ ảnh hưởng đến hoạt động của Ban; chỉ đạo phối hợp với Công an tỉnh, Sở Khoa học và Công nghệ, các cơ quan chuyên môn và đơn vị cung cấp dịch vụ khi có yêu cầu hoặc khi sự cố vượt khả năng xử lý của Ban.

2. Văn phòng Ban

- a) Là đầu mối tham mưu, theo dõi và đôn đốc việc triển khai Kế hoạch.
- b) Theo dõi hồ sơ, tài liệu liên quan đến công tác bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu.
- c) Tổng hợp, tham mưu báo cáo kết quả thực hiện Kế hoạch theo yêu cầu của cấp có thẩm quyền.

3. Chuyên viên công nghệ thông tin

- a) Là đầu mối chuyên môn kỹ thuật về an toàn thông tin của Ban.
- b) Chủ trì rà soát hiện trạng hệ thống mạng, thiết bị, phần mềm, tài khoản và các giải pháp bảo vệ hệ thống.
- c) Tham mưu hoàn thiện hồ sơ đề xuất cấp độ an toàn hệ thống thông tin; theo dõi việc khắc phục các yêu cầu liên quan đến cấp độ.
- d) Theo dõi cảnh báo an toàn thông tin; phối hợp xử lý lỗ hổng, mã độc và sự cố.
- đ) Hướng dẫn các phòng CMNV, người sử dụng thực hiện các yêu cầu về bảo mật tài khoản, thiết bị và dữ liệu.
- e) Chủ trì hoặc phối hợp thực hiện sao lưu, kiểm tra khả năng phục hồi dữ liệu thuộc phạm vi được giao.
- g) Phối hợp với Đội ứng cứu sự cố thông tin trong tiếp nhận, phân tích và xử lý sự cố.
- h) Tổng hợp các nguy cơ, lỗ hổng và đề xuất giải pháp kỹ thuật; tham mưu việc thuê dịch vụ, bảo trì, nâng cấp, gia hạn hoặc mua sắm giải pháp an toàn thông tin khi cần thiết.

4. Các phòng chuyên môn nghiệp vụ

- a) Trưởng phòng chịu trách nhiệm tổ chức thực hiện các yêu cầu về bảo mật thông tin, bảo vệ dữ liệu trong phạm vi phòng mình.
- b) Quản lý chặt chẽ hồ sơ, dữ liệu thuộc lĩnh vực phụ trách; chỉ chia sẻ thông tin cho đúng đối tượng, đúng thẩm quyền và đúng mục đích.
- c) Khi phát hiện nguy cơ hoặc sự cố phải thông báo ngay cho chuyên viên công nghệ thông tin và lãnh đạo phòng; không tự ý xử lý theo cách có thể làm mất dữ liệu hoặc dấu vết sự cố.

5. Viên chức, người lao động

- a) Chấp hành các quy định của Ban về sử dụng hệ thống thông tin, mạng máy tính, thiết bị công nghệ thông tin và dữ liệu.
- b) Bảo vệ tài khoản, mật khẩu, chữ ký số và các phương tiện xác thực được giao.

c) Không chia sẻ tài khoản, mật khẩu hoặc dữ liệu công việc cho người không có thẩm quyền.

d) Không tự ý cài đặt phần mềm, kết nối thiết bị hoặc sử dụng dịch vụ trực tuyến có nguy cơ ảnh hưởng đến an toàn thông tin và kịp thời báo cáo khi phát hiện dấu hiệu bất thường hoặc sự cố an toàn thông tin.

VI. CHẾ ĐỘ KIỂM TRA, BÁO CÁO

1. Các phòng CMNV báo cáo tình hình thực hiện nhiệm vụ được giao cho Văn phòng Ban.

2. Văn phòng Ban tổng hợp chung, tham mưu lãnh đạo Ban chỉ đạo xử lý và báo cáo theo quy định.

3. Chuyên viên công nghệ thông tin tổng hợp tình hình kỹ thuật, nguy cơ, lỗ hổng và sự cố. Đối với sự cố nghiêm trọng hoặc có nguy cơ ảnh hưởng đến hệ thống, dữ liệu, hoạt động của Ban, phải báo cáo ngay lãnh đạo Ban và phối hợp với cơ quan chuyên trách, đơn vị cung cấp dịch vụ để xử lý.

VII. TỔ CHỨC THỰC HIỆN

1. Trưởng các phòng CMNV căn cứ Kế hoạch này tổ chức triển khai đến viên chức, người lao động thuộc phạm vi quản lý; chịu trách nhiệm về kết quả thực hiện các nhiệm vụ được giao.

2. Văn phòng Ban chỉ đạo chuyên viên công nghệ thông tin theo dõi, đôn đốc và tổng hợp kết quả thực hiện Kế hoạch.

3. Chuyên viên công nghệ thông tin chủ trì tham mưu các giải pháp kỹ thuật, hướng dẫn thực hiện và phối hợp xử lý các nguy cơ, lỗ hổng, sự cố an toàn thông tin.

Trên đây là Kế hoạch triển khai công tác bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu năm 2026 của Ban QLDA. Trong quá trình tổ chức thực hiện, nếu phát sinh khó khăn, vướng mắc hoặc có nội dung cần điều chỉnh, bổ sung cho phù hợp với tình hình thực tế, các phòng CMNV kịp thời phản ánh về Văn phòng Ban để tổng hợp, tham mưu Giám đốc Ban xem xét, chỉ đạo thực hiện./.

Nơi nhận:

- Như trên;
- Lãnh đạo Ban;
- Các phòng CMNV;
- Trang thông tin điện tử Ban;
- Lưu: VT, VP.Tâm.

GIÁM ĐỐC



Trần Hoàng Vĩnh