

Số: 341 /KH-UBND

Phú Quốc, ngày 28 tháng 7 năm 2026

KẾ HOẠCH

Bảo đảm an toàn thông tin mạng và ứng phó sự cố an toàn thông tin của UBND đặc khu Phú Quốc năm 2026

Căn cứ Luật An ninh mạng ngày 10 tháng 12 năm 2025;

Căn cứ Luật chuyển đổi số ngày 11 tháng 12 năm 2025;

Căn cứ Công nghệ cao ngày 10 tháng 12 năm 2025;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng;

Căn cứ Nghị định số 47/2026/TT-BCA ngày 12/5/2026 của Bộ Công an về việc Ban hành quy chuẩn kỹ thuật Quốc gia về an ninh mạng cho Hệ thống thông tin lưu trữ tài liệu điện tử trong các cơ quan Đảng, Nhà nước;

Căn cứ Quyết định số 6901/QĐ-UBND ngày 17/10/2025 của UBND đặc khu về việc ban hành quy chế bảo đảm an toàn thông tin và bảo mật dữ liệu của Ủy ban nhân dân đặc khu Phú Quốc;

Căn cứ Quyết định số 10/QĐ-UBND ngày 07/01/2026 của UBND đặc khu về việc ban hành Phương án ứng phó sự cố an ninh mạng cho hệ thống thông tin của UBND đặc khu Phú Quốc, tỉnh An Giang;

Căn cứ Quyết định số 9470/QĐ-UBND ngày 26/6/2026 của UBND đặc khu về việc thành lập Đội ứng cứu an ninh mạng nội bộ của Ủy ban nhân dân đặc khu Phú Quốc.

UBND đặc khu xây dựng Kế hoạch bảo đảm an toàn thông tin mạng và ứng phó sự cố an toàn thông tin của UBND đặc khu Phú Quốc năm 2026 như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

Nâng cao hiệu quả công tác quản lý nhà nước về bảo đảm an toàn thông tin mạng tại UBND đặc khu và các cơ quan, đơn vị trực thuộc.

Chủ động phòng ngừa, phát hiện, xử lý kịp thời các nguy cơ mất an toàn thông tin; hạn chế thấp nhất nguy cơ mất dữ liệu, lộ lọt thông tin, gián đoạn hoạt động của các hệ thống thông tin phục vụ công tác chỉ đạo, điều hành và giải quyết thủ tục hành chính.

Nâng cao trách nhiệm của người đứng đầu, cán bộ, công chức, viên chức trong việc quản lý, khai thác và sử dụng hệ thống thông tin, thiết bị công nghệ thông tin theo đúng quy định.

Chủ động phối hợp với Công an tỉnh, Sở Khoa học và Công nghệ và các cơ quan liên quan trong công tác bảo đảm an toàn thông tin và ứng phó sự cố.

2. Yêu cầu

Thực hiện nghiêm các quy định của pháp luật về an toàn thông tin mạng, an ninh mạng và các quy định của UBND tỉnh, UBND đặc khu.

Bảo đảm các hệ thống thông tin, tài khoản, thiết bị công nghệ thông tin được quản lý, sử dụng đúng mục đích, an toàn, hiệu quả.

Chủ động phòng ngừa, sẵn sàng ứng phó, xử lý nhanh các sự cố an toàn thông tin phát sinh.

Thực hiện đầy đủ chế độ báo cáo, phối hợp và khắc phục các tồn tại theo yêu cầu của cơ quan có thẩm quyền.

II. NHIỆM VỤ

1. Tuyên truyền, nâng cao nhận thức

Tổ chức phổ biến các quy định của pháp luật về an toàn thông tin mạng, an ninh mạng đến cán bộ, công chức, viên chức và người lao động.

Tăng cường tuyên truyền về các nguy cơ mất an toàn thông tin, phương thức, thủ đoạn tấn công mạng; hướng dẫn kỹ năng sử dụng thư điện tử công vụ, chữ ký số, hệ thống thông tin và các nền tảng số an toàn.

Khuyến khích cán bộ, công chức tham gia các chương trình tập huấn, bồi dưỡng về an toàn thông tin do cấp trên tổ chức.

2. Rà soát, quản lý tài khoản và thiết bị

- Các cơ quan, đơn vị định kỳ rà soát việc quản lý, sử dụng:

+ Tài khoản thư điện tử công vụ.

+ Tài khoản Hệ thống quản lý văn bản và điều hành.

+ Tài khoản Hệ thống thông tin giải quyết thủ tục hành chính.

+ Chữ ký số chuyên dùng.

+ Các tài khoản truy cập hệ thống thông tin dùng chung của tỉnh.

- Đồng thời thực hiện:

+ Thu hồi tài khoản của cán bộ nghỉ việc, chuyển công tác.

+ Thay đổi mật khẩu định kỳ.

+ Không sử dụng chung tài khoản.

+ Không cung cấp tài khoản, mật khẩu cho người không có nhiệm vụ.

3. Quản lý, sử dụng thiết bị công nghệ thông tin

- Các cơ quan, đơn vị thực hiện:
- + Cập nhật hệ điều hành và phần mềm theo khuyến cáo của đơn vị quản lý.
- + Cài đặt và duy trì phần mềm phòng, chống mã độc.
- + Không cài đặt phần mềm không rõ nguồn gốc.
- + Không sử dụng phần mềm vi phạm bản quyền.
- + Hạn chế sử dụng thiết bị lưu trữ cá nhân để sao chép dữ liệu công vụ.
- + Quản lý chặt chẽ máy tính, thiết bị công nghệ thông tin được giao.

4. Bảo đảm an toàn dữ liệu

- Thực hiện sao lưu dữ liệu định kỳ đối với các dữ liệu thuộc phạm vi quản lý của đơn vị.
- Quản lý, khai thác và sử dụng dữ liệu đúng quy định.
- Không tự ý chia sẻ dữ liệu công vụ lên các nền tảng trực tuyến khi chưa được phép.
- Bảo đảm an toàn thông tin trong quá trình trao đổi, lưu trữ và xử lý dữ liệu.

5. Theo dõi, giám sát và xử lý cảnh báo

Thường xuyên theo dõi các cảnh báo, khuyến nghị về an toàn thông tin của cơ quan chuyên môn và đơn vị quản lý hệ thống; kịp thời rà soát, xử lý hoặc báo cáo khi phát hiện dấu hiệu mất an toàn thông tin.

6. Công tác ứng phó sự cố

- Khi xảy ra sự cố an toàn thông tin, các cơ quan, đơn vị có trách nhiệm:
- + Kịp thời cô lập thiết bị, hệ thống có dấu hiệu bị tấn công hoặc nhiễm mã độc.
- + Báo cáo ngay người đứng đầu đơn vị và Văn phòng HĐND và UBND đặc khu.
- + Phối hợp với Công an đặc khu, Công an tỉnh, Sở Khoa học và Công nghệ và đơn vị quản lý hệ thống để xử lý sự cố theo quy định.
- + Thực hiện việc khắc phục, phục hồi hoạt động của hệ thống theo Phương án ứng phó sự cố đã được UBND đặc khu ban hành.

7. Tự kiểm tra, rà soát

Văn phòng HĐND và UBND đặc khu chủ trì, phối hợp các cơ quan, đơn vị định kỳ rà soát việc thực hiện Quy chế bảo đảm an toàn thông tin; việc quản lý tài khoản, thiết bị, dữ liệu và việc thực hiện các quy định về bảo đảm an toàn thông tin tại các cơ quan, đơn vị; kịp thời nhắc nhở, hướng dẫn khắc phục các tồn tại, hạn chế.

III. TỔ CHỨC THỰC HIỆN

1. Văn phòng HĐND và UBND

- Chủ trì tham mưu UBND đặc khu triển khai thực hiện Kế hoạch này.

- Theo dõi, đôn đốc, hướng dẫn các cơ quan, đơn vị thực hiện các nhiệm vụ về bảo đảm an toàn thông tin và ứng phó sự cố.

- Chủ trì phối hợp với các cơ quan liên quan rà soát, tổng hợp tình hình bảo đảm an toàn thông tin; tham mưu UBND đặc khu báo cáo cơ quan có thẩm quyền theo quy định.

- Phối hợp với các cơ quan chuyên môn và đơn vị quản lý hệ thống thông tin của tỉnh trong việc xử lý các sự cố an toàn thông tin khi phát sinh.

- Theo dõi, đôn đốc việc khắc phục các tồn tại, hạn chế theo kết luận, kiến nghị của cơ quan có thẩm quyền.

2. Phòng Văn hóa - Xã hội

- Chủ trì tham mưu UBND đặc khu triển khai các nhiệm vụ về chuyển đổi số, bảo đảm an toàn thông tin theo chức năng, nhiệm vụ được giao.

- Phối hợp tuyên truyền, phổ biến các quy định của pháp luật.

- Chủ trì, phối hợp các đơn vị liên quan quản lý, hướng dẫn việc sử dụng thư điện tử công vụ, phần mềm Window, Office, chữ ký số chuyên dùng, các nền tảng số, hệ thống thông tin dùng chung và các ứng dụng phục vụ chuyển đổi số theo quy định.”

3. Trung tâm Phục vụ hành chính công

- Tổ chức thực hiện các biện pháp bảo đảm an toàn thông tin đối với Hệ thống thông tin giải quyết thủ tục hành chính, Trang Thông tin điện tử đặc khu và các thiết bị công nghệ thông tin được giao quản lý, sử dụng.

- Thực hiện quản lý, sử dụng tài khoản, chữ ký số, thư điện tử công vụ và các thiết bị phục vụ tiếp nhận, giải quyết thủ tục hành chính theo đúng quy định.

- Chủ động rà soát, sao lưu dữ liệu thuộc phạm vi quản lý; kịp thời phát hiện, báo cáo các nguy cơ, sự cố mất an toàn thông tin và phối hợp xử lý theo quy định.

- Phối hợp với Văn phòng HĐND và UBND đặc khu, Phòng Văn hóa - Xã hội, Công an đặc khu và các cơ quan liên quan trong việc triển khai các giải pháp bảo đảm an toàn thông tin tại Trung tâm.

4. Công an đặc khu

- Phối hợp tuyên truyền, hướng dẫn thực hiện các quy định của pháp luật về bảo đảm an ninh mạng, an toàn thông tin.

- Phối hợp rà soát, đánh giá nguy cơ mất an toàn thông tin; tham gia xử lý các sự cố an toàn thông tin theo thẩm quyền.

- Phối hợp với Công an tỉnh và các cơ quan chức năng trong công tác kiểm tra, hướng dẫn, xử lý các vụ việc liên quan đến an ninh mạng, an toàn thông tin khi có yêu cầu.

- Tham gia Đội ứng cứu sự cố an toàn thông tin của UBND đặc khu theo quy định.

5. Các cơ quan, đơn vị thuộc UBND đặc khu

- Tổ chức triển khai thực hiện nghiêm các nội dung của Kế hoạch này và các quy định về bảo đảm an toàn thông tin.
- Phân công cán bộ phụ trách hoặc đầu mối theo dõi công tác bảo đảm an toàn thông tin tại đơn vị.
- Quản lý chặt chẽ tài khoản, thiết bị, dữ liệu và việc sử dụng các hệ thống thông tin thuộc phạm vi quản lý; thực hiện sao lưu dữ liệu, thay đổi mật khẩu định kỳ và các biện pháp bảo đảm an toàn thông tin theo quy định.
- Kịp thời báo cáo Văn phòng HĐND và UBND đặc khu khi phát hiện nguy cơ hoặc xảy ra sự cố mất an toàn thông tin; phối hợp với các cơ quan, đơn vị liên quan để xử lý, khắc phục.
- Thực hiện đầy đủ chế độ báo cáo và khắc phục các tồn tại, hạn chế theo yêu cầu của cơ quan có thẩm quyền.

6. Chế độ báo cáo

Các cơ quan, đơn vị định kỳ (**6 tháng và năm**) hoặc đột xuất báo cáo tình hình thực hiện công tác bảo đảm an toàn thông tin và ứng phó sự cố về Văn phòng HĐND và UBND đặc khu để tổng hợp, tham mưu UBND đặc khu báo cáo cơ quan có thẩm quyền.

Trên đây là Kế hoạch bảo đảm an toàn thông tin mạng và ứng phó sự cố an toàn thông tin của UBND đặc khu Phú Quốc năm 2026./. *Hua*

Nơi nhận:

- Phòng An ninh mạng, Công an tỉnh (để b/c);
- Lãnh đạo UBND đặc khu;
- Các phòng, ban, đơn vị thuộc UBND đặc khu;
- Công an đặc khu;
- Trang thông tin điện tử đặc khu;
- Lưu: VT, ttsi.



**KT. CHỦ TỊCH
PHÓ CHỦ TỊCH**

luu
Nguyễn Thị Kim Loan