TIỂU BAN AN NINH MẠNG KHÁNH HÒA
CƠ QUAN THƯỜNG TRỰC

Số: 5957 /KH-CQTTTB

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

Khánh Hòa, ngày 19 tháng 11 năm 2025

KẾ HOẠCH
Kiểm tra, đánh giá công tác bảo đảm an ninh mạng đối với các hệ thống thông tin quan trọng trên địa bàn tỉnh

Căn cứ Chỉ thị số 09/CT-TTg ngày 23/02/2024 của Thủ tướng Chính phủ về tuân thủ quy định pháp luật và tăng cường thực hiện công tác bảo đảm an toàn đối với các hệ thống thông tin theo cấp độ;

Căn cứ chỉ đạo của Tỉnh ủy Khánh Hòa tại công văn số 4148-CV/TU ngày 02/4/2025 về việc rà soát, bảo đảm an toàn, an ninh mạng đối với các hệ thống thông tin của các cơ quan Đảng;

Căn cứ chỉ đạo của UBND tỉnh tại công văn số 1184/UBND-NC ngày 30/7/2025 về tăng cường thực hiện các biện pháp bảo đảm an toàn thông tin mạng trong quá trình triển khai mô hình chính quyền địa phương 02 cấp;

Thực hiện Công điện số 232/CĐ-TTg ngày 21/9/2025 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng, bảo mật dữ liệu cho các hệ thống công nghệ thông tin;

Nhằm đảm bảo an ninh an toàn thông tin sau khi thực hiện sắp xếp đơn vị hành chính và xây dựng chính quyền địa phương 02 cấp trên địa bàn tỉnh, Công an tỉnh – Cơ quan Thường trực Tiểu ban An ninh mạng tỉnh Khánh Hòa ban hành Kế hoạch kiểm tra, đánh giá việc bảo đảm an toàn, an ninh mạng đối với hệ thống thông tin quan trọng trên địa bàn tỉnh Khánh Hòa năm 2025, cụ thể như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Nhằm thực hiện hiệu quả công tác bảo đảm an toàn thông tin mạng của các cơ quan Đảng, Nhà nước trên địa bàn tỉnh, nâng cao khả năng thích ứng một cách chủ động, linh hoạt và giảm thiểu các nguy cơ gây mất an ninh, an toàn thông tin mạng; triển khai toàn diện, đồng bộ các biện pháp, giải pháp để phòng ngừa và kịp thời ứng phó, khắc phục khi có sự cố về an toàn thông tin mạng.

- Nâng cao vai trò, nhận thức của người đứng đầu các Đảng ủy trực thuộc Tỉnh ủy, lãnh đạo các sở, ban, ngành, UBND các xã, phường, đặc khu đối với công tác bảo

đảm an toàn thông tin trong các hoạt động ứng dụng công nghệ thông tin (CNTT) của cơ quan Nhà nước. Chú trọng việc thường xuyên quán triệt, nâng cao nhận thức đối với các cán bộ, công chức, viên chức, người lao động tại đơn vị tuân thủ đúng các quy định trong quá trình khai thác, vận hành hệ thống thông tin, giảm thiểu nguy cơ, thiệt hại do mất an toàn hệ thống mạng; kịp thời có biện pháp phòng ngừa, ngăn chặn xảy ra sự cố bí tấn công mạng, gián điệp mạng, lộ, mất bí mật nhà nước trên không gian mạng.

- Kiểm tra, đánh giá thực trạng công tác bảo đảm an toàn an ninh mạng đối với: [1]Hạ tầng hệ thống mạng và các máy vi tính có kết nối vào hệ thống mạng diện rộng của Trung tâm Dữ liệu tỉnh (*đặc biệt là các máy vi tính có tài khoản truy cập, khai thác vào hệ thống cơ sở dữ liệu quốc gia về dân cư*); [2]Việc nghiên cứu, đề xuất và xác định cấp độ đối với các hệ thống thông tin quan trọng thuộc cơ quan Đảng, Nhà nước chủ quản/ quản lý/ vận hành theo quy định và công tác quản lý tài liệu, dữ liệu điện tử nội bộ chứa thông tin nhạy cảm, quan trọng trong hệ thống mạng (*kể cả các "tệp tin" có nội dung chứa bí nhà nước*); [3]Chất lượng hoạt động và tiêu chuẩn bảo đảm an toàn thông tin của các cổng/trang thông tin điện tử và các hệ thống phần mềm ứng dụng chuyên ngành mà đơn vị đang quản lý, khai thác sử dụng.

- Nắm bắt thực trạng, đánh giá hiệu quả thực tế đối với công tác triển khai các biện pháp đảm bảo an ninh, an toàn thông tin cho các hệ thống thông tin thuộc quản lý của cơ quan Đảng, Nhà nước trên địa bàn tỉnh Khánh Hòa sau khi thực hiện mô hình chính quyền địa phương 02 cấp; từ đó làm cơ sở để xây dựng phương án đảm bảo an toàn hệ thống thông tin theo cấp độ của tỉnh phù hợp các quy định tại 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 trong những năm tiếp theo.

2. Yêu cầu

Việc kiểm tra, đánh giá sự tuân thủ quy định về bảo đảm an toàn thông tin mạng, các hệ thống thông tin trên địa bàn tỉnh năm 2025 phải đảm bảo các yêu cầu sau:

- Kiểm tra, đánh giá việc đảm bảo tính tổng thể, chi tiết, đánh giá đúng thực trạng an toàn thông tin tại các đơn vị được kiểm tra, đánh giá; từ đó có kiến nghị, hướng dẫn khắc phục các điểm yếu, lỗ hổng bảo mật hệ thống.

- Quá trình kiểm tra, đánh giá không làm ảnh hưởng, gián đoạn các hoạt động của hệ thống thông tin của đơn vị được kiểm tra; đảm bảo tính bí mật thông tin kiểm tra, thực hiện đúng quy trình kiểm tra.

- Đảm bảo lựa chọn, thuê chuyên gia, cán bộ kỹ thuật thực hiện kiểm tra, đánh giá, hướng dẫn đáp ứng các yêu cầu chuyên môn, năng lực, kinh nghiệm về bảo mật, an ninh an toàn hệ thống mạng.

II. ĐỐI TƯỢNG, NỘI DUNG, QUY TRÌNH, THỜI GIAN KIỂM TRA

1. Đối tượng kiểm tra

1.1. Cơ quan Đảng, Nhà nước, sở, ban, ngành, đơn vị hiện chủ quản/ quản lý/ vận hành Hệ thống thông tin được phê duyệt cấp độ đã được thẩm định trước đây theo Nghị định số 85/2016/NĐ-CP của Chính phủ (cấp độ từ 1 đến 3).

1.2. Các sở, ban, ngành, đơn vị hiện đang chủ quản/ quản lý/ vận hành Hệ thống thông tin nhưng chưa làm hồ sơ đề xuất phê duyệt cấp độ theo chỉ đạo của UBND tỉnh tại Công văn số 3856/UBND-NC&KSTT ngày 08/4/2025.

1.3. Doanh nghiệp nhà nước, đơn vị sự nghiệp và các nhà cung cấp dịch vụ viễn thông, internet hiện đang chủ quản/ quản lý/ vận hành các hệ thống thông tin quan trọng, lưu trữ và xử lý dữ liệu nhạy cảm của cá nhân, tổ chức trên địa bàn tỉnh.

2. Nội dung kiểm tra

2.1. Việc thực hiện 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 và Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP của Chính phủ gồm: (1)Kiểm tra công tác lập hồ sơ, trình phê duyệt cấp độ đối với các hệ thống thông tin thuộc cơ quan Đảng, Nhà nước chủ quản/ quản lý/ vận hành; (2)Kiểm tra việc thiết lập và triển khai các phương án đảm bảo an toàn an ninh mạng đối với các hệ thống thông tin quan trọng.

2.2. Công tác lãnh đạo, chỉ đạo thực hiện rà soát, bảo đảm an toàn, an ninh mạng đối với các hệ thống thông tin của Tỉnh ủy, UBND tỉnh trong quá trình triển khai thực hiện mô hình chính quyền địa phương 02 cấp[1]; đặc biệt là kiểm tra thực tế việc bàn giao, lưu trữ và xử lý chuyển giao tài liệu, dữ liệu điện tử trên các trang thiết bị chuyên dụng.

2.3. Kiểm tra, đánh giá thực tế việc đảm bảo an toàn, an ninh thông tin mạng

---

[1] Công văn số 1256/UBND-NC v/v triển khai thực hiện đồng bộ các biện pháp bảo đảm an toàn thông tin mạng; Công văn số 2579/UBND-NC&KSTT v/v thực hiện các giải pháp bảo đảm an toàn thông tin mạng trong giai đoạn chuyển giao nhiệm vụ; Công văn số 3856/UBND-NC v/v tăng cường các biện pháp bảo đảm an toàn thông tin mạng trong giai đoạn sắp xếp, tổ chức bộ máy; Công văn số 5479/UBND-NC ngày 08/5/2025 ban hành Kế hoạch Ứng phó sự cố an toàn thông tin mạng trên địa bàn tỉnh Khánh Hòa; Công văn số 6606/CV-CAT(ANM) ngày 28/6/2025 thực hiện hiệu quả công tác bảo vệ an toàn an ninh mạng cho hoạt động của mô hình chính quyền địa phương 02 cấp.

máy tính và các hệ thống thông tin của cơ quan đơn vị và công tác giám sát, quản lý, hướng dẫn của cán bộ phụ trách quản trị vận hành hệ thống thông tin.

2.4. Kiểm tra công tác đào tạo, tập huấn, nâng cao nhận thức của cán bộ, công chức, viên chức về công tác đảm bảo an toàn thông tin và công tác bảo vệ bí mật nhà nước trên không gian mạng.

2.5. Kiểm tra, đánh giá chất lượng hoạt động của các trang/cổng thông tin điện tử thuộc cơ quan Đảng, Nhà nước chủ quản/ quản lý/ vận hành và việc chấp hành các quy định về soạn thảo, kiểm duyệt nội dung, đăng tải thông tin.

3. Quy trình kiểm tra

- Đơn vị được kiểm tra chủ động thực hiện rà soát, xây dựng báo cáo theo nội dung tại đề cương báo cáo chi tiết trong Kế hoạch *(đề cương báo cáo chi tiết theo Phụ lục gửi kèm).*

- Đoàn kiểm tra tổ chức kiểm tra thực tế, rà quét nhằm phát hiện các lỗ hổng về an toàn thông tin đối với hệ thống mạng, các máy vi tính tại cơ quan, đơn vị, địa phương và đơn vị trực thuộc trong phạm vi kiểm tra.

- Đoàn kiểm tra thông báo kết quả kiểm tra, kiến nghị những vấn đề cần khắc phục, hướng dẫn các biện pháp phát huy hiệu quả hoạt động đảm bảo an toàn thông tin mạng, phòng chống tấn công mạng, gián điệp mạng đối với các hệ thống thông tin quan trọng được phê duyệt cấp độ tại cơ quan, đơn vị.

- Đoàn kiểm tra và đơn vị được kiểm tra tiến hành lập biên bản kiểm tra và các biểu mẫu thống kê, đánh giá thực trạng công tác tuân thủ quy định về bảo đảm an toàn an ninh mạng đối với các hệ thống thông tin quan trọng trên địa bàn tỉnh, cùng thống nhất các nội dung trong biên bản để Đoàn kiểm tra tổng hợp kết quả, báo cáo đồng chí Trưởng Tiểu ban An ninh mạng tỉnh.

4. Thời gian kiểm tra

- Thời gian kiểm tra: Dự kiến trong Quý IV năm 2025 và Quý I năm 2026; khi kết thúc kiểm tra, Đoàn kiểm tra sẽ tập hợp kết quả báo cáo Tỉnh ủy, UBND tỉnh.

- Đoàn kiểm tra sẽ thông báo lịch cụ thể đến các đơn vị, địa phương.

III. THÀNH PHẦN ĐOÀN KIỂM TRA

1. Phó Giám đốc Công an tỉnh, Cơ quan Thường trực Tiểu ban An ninh mạng tỉnh - Trưởng đoàn.

2. Lãnh đạo Văn phòng Tiểu ban An ninh mạng tỉnh - Phó Trưởng đoàn.

3. Cán bộ Cơ quan Thường trực Tiểu ban An ninh mạng tỉnh: 05 người.

4. Chuyên viên Sở Khoa học & Công nghệ: 02 người.

IV. KINH PHÍ

Thực hiện theo Quyết định số 3321/QĐ-UBND ngày 23/12/2024 của UBND tỉnh Khánh Hòa về việc giao chỉ tiêu kế hoạch và dự toán ngân sách nhà nước năm 2025 cho Công an tỉnh Khánh Hòa.

V. TỔ CHỨC THỰC HIỆN

1. Công an tỉnh - Cơ quan Thường trực Tiểu ban An ninh mạng tỉnh

- Chủ trì tổ chức triển khai thực hiện Kế hoạch, chuẩn bị các điều kiện cần thiết để phục vụ công tác kiểm tra; thành lập Đoàn kiểm tra và thông báo lịch kiểm tra đến các cơ quan, đơn vị, địa phương được kiểm tra để chuẩn bị các nội dung làm việc, báo cáo theo Kế hoạch.

- Tổ chức kiểm tra, rà quét việc đảm bảo an toàn thông tin đối với các cổng/trang thông tin điện tử thuộc cơ quan, đơn vị được kiểm tra theo đề nghị của Đoàn kiểm tra *(trước khi Đoàn tiến hành làm việc trực tiếp)*.

- Thực hiện kiểm tra, đánh giá các nội dung tại Phần II của Phụ lục kèm theo Kế hoạch này.

- Tổng hợp, đánh giá, thông báo kết quả kiểm tra; báo cáo, tham mưu, kiến nghị các nội dung có liên quan thuộc thẩm quyền của Tỉnh ủy, UBND tỉnh theo quy định.

2. Sở Khoa học & Công nghệ

- Bố trí cán bộ có chuyên môn về an toàn thông tin mạng phối hợp với Công an tỉnh rà soát, kiểm duyệt danh sách các hệ thống thông tin được phê duyệt cấp độ; đánh giá nguy cơ bị tấn công mạng đối với các hệ thống thông tin, phần mềm ứng dụng dịch vụ, cổng/ trang thông tin điện tử được bố trí hạ tầng mạng trong Trung tâm Dữ liệu tỉnh; đồng thời thực hiện đối soát các trang, thiết bị hạ tầng mạng theo đúng thực tế, phù hợp với mô hình tham chiếu, đặc biệt là đối với các thành phần hệ thống có kết nối/ đặt máy chủ tại Trung tâm Dữ liệu tỉnh.

- Phối hợp với Công an tỉnh thực hiện kiểm tra, đánh giá đối với các nội dung tại Phần II của Phụ lục đính kèm theo Kế hoạch này.

3. Các cơ quan, đơn vị, địa phương được kiểm tra

- Các cơ quan, đơn vị, địa phương được kiểm tra, đánh giá chủ động bố trí, phân công người có thẩm quyền/ trách nhiệm tham gia làm việc với Đoàn kiểm tra; cung cấp thông tin liên hệ cán bộ phụ trách lĩnh vực công nghệ thông tin, an toàn thông tin mạng và chuyên viên quản trị, vận hành hệ thống thông tin; chuẩn bị Báo

cáo phục vụ Đoàn kiểm tra *(theo mẫu báo cáo chi tiết tại Phụ lục gửi kèm)* gửi về Công an tỉnh - Cơ quan Thường trực Tiểu ban An ninh mạng tỉnh 03 ngày trước thời điểm kiểm tra tại đơn vị, địa phương theo Kế hoạch.

- Trong quá trình thực hiện nếu có vấn đề phát sinh vượt thẩm quyền, Công an tỉnh tổng hợp, báo cáo UBND tỉnh để xem xét, quyết định./.

Nơi nhận:
- Đ/c Trưởng Tiểu ban ANM tỉnh (báo cáo);
- Đ/c Giám đốc Công an tỉnh (báo cáo);
- Các sở, ban, ngành, đơn vị liên quan;
- Đảng ủy, UBND các xã, phường;
- Lưu: VT, ANM.

TM. CƠ QUAN THƯỜNG TRỰC
TIỂU BAN AN NINH MẠNG TỈNH

CÔNG HÒA X.H.C.N VIỆT NAM
CÔNG AN TỈNH KHÁNH HÒA

Đại tá Nguyễn Đình Thuận Hải
PHÓ GIÁM ĐỐC CÔNG AN TỈNH

PHỤ LỤC
ĐỀ CƯƠNG BÁO CÁO CHI TIẾT

(Kèm theo Kế hoạch số 5957/KH-CQTTTB ngày 19/11/2025 của Công an tỉnh - Cơ quan Thường trực Tiểu ban An ninh mạng tỉnh Khánh Hòa)

I. THÔNG TIN CHUNG CỦA ĐƠN VỊ ĐƯỢC KIỂM TRA

1. Đơn vị được kiểm tra chuẩn bị Báo cáo các nội dung

- Tình hình ứng dụng công nghệ thông tin của cơ quan, đơn vị, địa phương;

- Tình hình chung công tác đảm bảo an toàn thông tin mạng và bảo vệ bí mật nhà nước trên không gian mạng;

- Tình hình bố trí nhân lực chuyên trách/bán chuyên trách về công nghệ thông tin, an toàn thông tin;

- Ngân sách đã bố trí chi cho công tác bảo đảm an toàn thông tin mạng.

2. Tài liệu, văn bản của đơn vị cần cung cấp cho Đoàn kiểm tra

- Bộ quy trình vận hành hệ thống thông tin, sao lưu dữ liệu, xử lý sự cố; giám sát nhật ký hoạt động; quy định về phạm vi, quyền hạn, trách nhiệm của người sử dụng, vận hành, quản trị hệ thống.

- Bộ tài liệu hướng dẫn sử dụng các phần mềm nghiệp vụ; văn bản danh sách các tài khoản được phép truy cập vào hệ thống; có phân quyền quản trị, chức năng được phép khai thác cụ thể đối với từng tài khoản người dùng.

- Tài liệu thể hiện sơ đồ tổng thể hệ thống, số lượng đường truyền internet riêng biệt, phân vùng mạng theo chức năng riêng (có địa chỉ IP cụ thể từng vùng độc lập), danh sách số lượng máy vi tính được kết nối vào hệ thống mạng nội bộ, internet chuyên dùng; máy chủ, các thiết bị mạng chuyên dụng khác (nếu có).

II. NỘI DUNG KIỂM TRA, ĐÁNH GIÁ

1. Việc thực hiện 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 và Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều đối với Nghị định số 85.

2. Công tác lãnh đạo, chỉ đạo về an toàn thông tin mạng;

3. Công tác lập hồ sơ đề xuất phê duyệt cấp độ toàn thông tin đối với các hệ thống thông tin đang chủ quản/ quản lý, vận hành;

4. Việc xây dựng và triển khai các phương án đảm bảo an toàn hệ thống thông tin;

5. Việc thực hiện, ban hành quy chế, quy định về đảm bảo an toàn thông tin

trong nội bộ cơ quan, đơn vị, địa phương; tuyên truyền, triển khai các nội dung theo quy chế;

6. Công tác tổ chức thực thi và kiểm tra đôn đốc thực hiện các quy định của pháp luật về bảo đảm an toàn, an ninh mạng; chủ động tự rà soát, thực hiện kiểm tra đánh giá tổng thể về an toàn thông tin theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ;

7. Việc thực hiện Chỉ thị số 14/CT-TTg ngày 07/6/2019 của Thủ tướng Chính phủ về việc tăng cường công tác bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam.

8. Công tác tổ chức tuyên truyền, tập huấn nâng cao nhận thức, trách nhiệm về an toàn thông tin mạng, các kỹ năng phòng chống, xử lý các mối nguy hại của virus, mã độc; các phương thức thực hiện tấn công mạng, gián điệp mạng.

9. Tình hình sử dụng và quản lý khóa bí mật (USB token) của chữ ký số, dịch vụ chứng thực chữ ký số chuyên dùng của Chính phủ;

10. Công tác bố trí nhân lực đảm bảo cho an toàn thông tin mạng.

11. Kiểm tra toàn diện thực trạng, công tác bảo đảm an toàn an ninh mạng.

- Chất lượng hoạt động của hệ thống mạng LAN, WAN.

- Tình hình hoạt động của trang thiết bị được đầu tư, hiện có trong hệ thống.

- Chất lượng băng thông dịch vụ mạng và đường truyền số liệu chuyên dùng.

- Việc thực hiện triển khai các giải pháp, trang thiết bị bảo mật và các phần mềm phòng chống mã độc/antivirus đối với hệ thống.

- Rà quét, đánh giá điểm yếu, lỗ hổng bảo mật của hệ thống cổng/trang thông tin điện tử *(được thực hiện bằng các phần mềm chuyên dụng, diễn ra ngoài giờ hành chính, có thông báo thời gian cụ thể để đơn vị được kiểm tra chủ động chuẩn bị).*

- Kiểm tra việc vận hành, quản trị hệ thống mạng nội bộ, mạng internet; quản lý, giám sát các tài khoản người dùng được cấp phát để truy cập, khai thác vào hệ thống thông tin dùng chung của tỉnh (E-Office, Giải quyết TTHC trực tuyến).

- Kiểm tra thực tế công tác bảo đảm an toàn thông tin và bảo vệ các tài liệu, dữ liệu điện tử chứa thông tin nội bộ/ nhạy cảm/ bí mật nhà nước trên hệ thống mạng; tiến hành hướng dẫn khắc phục/ xử lý vi phạm (*nếu phát hiện*).

- Kiểm tra công tác đào tạo, bồi dưỡng, tập huấn cán bộ, công chức, viên chức về công tác bảo đảm an toàn thông tin và bảo vệ bí mật nhà nước trên không gian mạng.

- Kiểm tra công tác quản lý, vận hành, thực hiện biện pháp kỹ thuật nhằm đáp

ứng đầy đủ yêu cầu cơ bản về bảo đảm an toàn hệ thống thông tin theo đúng cấp độ *(quy định tại Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022, tiêu chuẩn TCVN 11930:2017).*

- Kiểm tra thực tế công tác lưu trữ, bàn giao, xử lý thiết bị, dữ liệu điện tử trong quá trình sắp xếp, tổ chức bộ máy sau khi sáp nhập.

* Đề nghị các đơn vị có những sự thay đổi/ bổ sung/ tích hợp hệ thống thông tin đang chủ quản/ quản lý/ vận hành sau khi giải thể/ sáp nhập khẩn trương xây dựng hoàn thiện báo cáo thực trạng theo Đề cương chi tiết gửi kèm Công văn số 1184/UBND-NC ngày 30/7/2025 của UBND tỉnh về việc tăng cường thực hiện các biện pháp bảo đảm an toàn thông tin mạng trong quá trình triển khai mô hình chính quyền địa phương 02 cấp.

III. KHÓ KHĂN, VƯỚNG MẮC

IV. KIẾN NGHỊ, ĐỀ XUẤT