

TIỂU BAN AN NINH MẠNG
TỈNH KHÁNH HÒA
CƠ QUAN THƯỜNG TRỰC

Số 7175 /CV-CQTTTB

V/v triển khai thực hiện công
tác bảo đảm an ninh mạng, an
ninh thông tin, an ninh dữ liệu

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

Khánh Hòa, ngày 23 tháng 6 năm 2026

Kính gửi:

- Văn phòng Tỉnh ủy Khánh Hòa;
- Văn phòng UBND tỉnh Khánh Hòa;
- Các cơ quan tham mưu, giúp việc Tỉnh ủy;
- Các Đảng ủy trực thuộc Tỉnh ủy;
- Các Đảng ủy xã, phường, đặc khu;
- Ủy ban MTTQ Việt Nam tỉnh;
- Ủy ban MTTQ Việt Nam xã, phường, đặc khu;
- Các Sở, ban, ngành;
- Các đơn vị sự nghiệp trực thuộc UBND tỉnh;
- UBND xã, phường, đặc khu; cơ quan ngành dọc.

Căn cứ Công văn số 2656/BCA-A05 ngày 02/6/2026 của Bộ Công an về việc hướng dẫn triển khai công tác bảo đảm an ninh mạng, an ninh thông tin, an ninh dữ liệu, đặc biệt là đối với tiêu chuẩn quốc gia “TCVN 14423:2025 An ninh mạng - Yêu cầu đối với hệ thống thông tin quan trọng” (sau đây viết tắt là TCVN 14423:2025);

Thực hiện ý kiến chỉ đạo của UBND tỉnh tại Công văn số 7359/UBND-KGVX ngày 08/6/2026 về việc giao Công an tỉnh chủ trì, phối hợp các cơ quan liên quan rà soát, triển khai công tác bảo đảm an ninh mạng, an ninh thông tin, an ninh dữ liệu trên địa bàn tỉnh, với vai trò Cơ quan Thường trực Tiểu ban An ninh mạng, Công an tỉnh đề nghị các cơ quan, sở, ban, ngành, đơn vị, địa phương, đặc biệt là Văn phòng Tỉnh ủy, Văn phòng UBND tỉnh, Sở Khoa học & Công nghệ khẩn trương tổ chức nghiên cứu, phân tích, tham chiếu tiêu chuẩn quốc gia TCVN 14423:2025 làm cơ sở đánh giá tổng thể về an ninh mạng, bảo mật thông tin, an ninh dữ liệu và cập nhật, bổ sung chính sách quản lý, quy trình quản trị, giải pháp bảo đảm an ninh mạng cho các hệ thống thông tin¹ trọng yếu trên địa bàn tỉnh.

Về việc này, Công an tỉnh đã nghiên cứu, triển khai một số nội dung trọng tâm đối với tiêu chuẩn quốc gia TCVN 14423:2025 và cảnh báo các nguy cơ về an ninh dữ liệu, cụ thể như sau:

¹ Thay thế cho Thông tư số 2009/TB-A05-TTANMQG ngày 11/4/2024 của Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao về việc hướng dẫn các biện pháp tăng cường bảo đảm an ninh mạng cho hệ thống thông tin quan trọng về an ninh quốc gia.

I. CÁC NỘI DUNG TRỌNG TÂM (THEO TIÊU CHUẨN TCVN 14423:2025 AN NINH MẠNG - YÊU CẦU ĐỐI VỚI HỆ THỐNG THÔNG TIN QUAN TRỌNG)

1. Xác định và phân loại tài sản² trong hệ thống thông tin: Thực hiện rà soát, lập danh mục tất cả tài sản phần cứng, phần mềm, dữ liệu trong hệ thống thông tin. Trong đó, nghiên cứu, đánh giá mức độ quan trọng của từng tài sản làm cơ sở xây dựng và triển khai phương án đảm bảo an ninh mạng cho hệ thống thông tin theo nguyên tắc “bảo vệ đúng, đầu tư đủ” không đầu tư lại các hệ thống hoặc thành phần hệ thống đã được đầu tư; xây dựng các hệ thống có khả năng khai thác, sử dụng các dữ liệu chia sẻ, dùng chung; phân bổ nguồn lực khoa học, tối ưu, tránh gây lãng phí.

2. Xác định và chuẩn hóa mô hình³ hệ thống thông tin: Tiến hành rà soát, cập nhật sơ đồ logic và vật lý của hệ thống thông tin, đảm bảo hệ thống được thiết kế theo nguyên tắc **phân chia vùng mạng⁴** theo hồ sơ đề xuất cấp độ, dựa theo chức năng và tuân thủ nguyên tắc “đặc điểm tối thiểu”, hạn chế tối đa bề mặt tấn công, ngăn chặn rủi ro lây lan khi có sự cố xảy ra.

3. Cấu hình bảo mật, rà soát, bóc gỡ mã độc và cập nhật bản vá: Thực hiện kiểm tra, đánh giá và **cấu hình bảo mật⁵** toàn bộ các tài sản trong hệ thống thông tin, thứ tự ưu tiên thực hiện dựa theo mức độ quan trọng của tài sản. Khẩn trương cài đặt đầy đủ phần mềm phòng, chống mã độc, rà quét, bóc gỡ triệt để mã độc trong hệ thống thông tin, đồng thời cập nhật các bản vá của hệ điều hành, ứng dụng đối với các lỗ hổng bảo mật đã được công bố.

² **Xác định tài sản:** Là quá trình rà soát, nhận diện và lập danh mục kiểm kê toàn bộ các tài sản thuộc hoặc có liên quan đến hệ thống thông tin của tổ chức. Quá trình này giúp tổ chức trả lời được câu hỏi: "Chúng ta đang sở hữu những thiết bị, phần mềm hay dữ liệu gì và chúng nằm ở đâu?"; **Phân loại tài sản:** Là việc đánh giá, gán nhãn và phân nhóm các tài sản đã được xác định dựa trên giá trị, tầm quan trọng hoặc mức độ nhạy cảm của chúng đối với hoạt động của tổ chức. Mục tiêu của phân loại là để thực hiện nguyên tắc "bảo vệ đúng, đầu tư đủ", tránh lãng phí nguồn lực bảo mật vào những tài sản không quan trọng và tập trung bảo vệ các tài sản cốt lõi. Dựa trên cấu trúc hệ thống thông tin, các tài sản thường được chia thành 3 nhóm lớn chính: Tài sản phần cứng, tài sản phần mềm, tài sản thông tin/dữ liệu.

³ **Chuẩn hóa mô hình:** Đây là quá trình rà soát, điều chỉnh và thống nhất cấu trúc kiến trúc của hệ thống thông tin (bao gồm cả mặt vật lý như thiết bị phần cứng, đường truyền và mặt logic như luồng dữ liệu, phân vùng mạng, quyền truy cập) để đưa hệ thống về một mẫu chuẩn quy chuẩn và an toàn.

⁴ **Vùng mạng biên:** Vùng mạng được thiết lập để cung cấp các kết nối hệ thống ra bên ngoài internet và các mạng khác. Vùng mạng này bao gồm các cặp Core Switch, Firewall chạy HA với nhau, được thiết lập để cung cấp các kết nối hệ thống ra bên ngoài internet và các mạng khác; **Vùng DMZ:** là vùng mạng được thiết lập để đặt các máy chủ công cộng, cho phép truy cập trực tiếp từ các mạng bên ngoài và mạng internet (thiết bị VPN, các máy chủ ứng dụng, dịch vụ Web, Email... phục vụ người dùng từ bên ngoài internet); **Vùng máy chủ nội bộ:** là vùng mạng bao gồm các máy chủ Web, máy chủ ứng dụng, AD, File Server... phục vụ cho người dùng trong nội bộ; **Vùng máy chủ cơ sở dữ liệu:** là vùng mạng được thiết lập để đặt các máy chủ cơ sở dữ liệu. Vùng này bao gồm các máy chủ chứa cơ sở dữ liệu (CSDL) của các ứng dụng trong hệ thống như: MySQL, Oracle, MSSQL, MongoDB...; **Vùng mạng nội bộ:** là vùng mạng này được thiết lập để cung cấp kết nối mạng cho các máy trạm và các thiết bị đầu cuối và các thiết bị khác của người sử dụng vào hệ thống, vùng mạng này có thể chia nhỏ thành vùng mạng theo phòng ban hoặc theo chức năng, nhiệm vụ...; **Vùng mạng không dây:** là vùng mạng không dây cần được tách riêng, độc lập với các vùng mạng khác: Bao gồm các Access point và Wifi Controller để quản lý các Access point; **Vùng hệ thống dự phòng:** là vùng mạng bao gồm các máy chủ vật lý, thiết bị tối thiểu để phục vụ khôi phục hệ thống khi xảy ra sự cố. Vùng hệ thống dự phòng phải được tác biệt hoàn toàn với hệ thống chính về mặt logic: ngắt kết nối vật lý hoặc được cô lập/cách ly bằng các thiết bị kiểm soát truy cập.

⁵ **Cấu hình bảo mật cho phần cứng và phần mềm** là thiết lập và duy trì cấu hình an toàn cho phần cứng như thiết bị người dùng cuối bao gồm máy tính, thiết bị di động và cảm tay, thiết bị mạng, thiết bị OT/IoT, máy chủ... và phần mềm như hệ điều hành, ứng dụng. Trong đó ưu tiên thiết lập và duy trì quy định, quy trình cấu hình an toàn cho tài sản phần cứng và phần mềm; cấu hình tự động khóa phiên làm việc trên các tài sản phần cứng và phần mềm. Đối với các phần mềm thuê khoán phải có biên bản, hợp đồng và cam kết bảo mật đối với bên thuê khoán các nội dung liên quan đến phát triển phần mềm thuê khoán và yêu cầu cung cấp mã nguồn phần mềm.

4. Triển khai, kết nối giám sát an ninh mạng: Thiết lập và duy trì giải pháp giám sát an ninh mạng tập trung, liên tục 24/7 đối với toàn bộ lưu lượng, sự kiện và nhật ký phần cứng, phần mềm trong hệ thống thông tin, đảm bảo khả năng phát hiện sớm, cảnh báo kịp thời các dấu hiệu bất thường, hành vi xâm nhập trái phép tác động tiêu cực đến hệ thống thông tin. Thực hiện kết nối hệ thống giám sát an ninh mạng về Trung tâm An ninh mạng quốc gia (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an) hoặc Trung tâm An ninh mạng địa phương⁶ để chia sẻ thông tin cảnh báo, hỗ trợ giám sát an ninh mạng, kịp thời phát hiện, ngăn chặn các mối đe dọa trên không gian mạng.

5. Rà soát, cập nhật, quy trình, quy định quản lý, vận hành hệ thống thông tin, đảm bảo an ninh mạng, an ninh an toàn dữ liệu, nâng cao năng lực, trình độ của cán bộ, nhân viên quản trị, vận hành, khai thác hệ thống thông tin:

- Tập trung kiện toàn tổ chức, nhân sự và chính sách nội bộ⁷, khẩn trương ban hành các quy chế bảo mật, làm rõ quyền hạn, trách nhiệm của từng cá nhân tham gia quản trị, vận hành, khai thác và bảo vệ hệ thống thông tin⁸, an ninh an toàn dữ liệu⁹. Đồng thời, tổ chức đào tạo nâng cao chuyên môn, nhận thức đảm bảo an ninh mạng cho toàn thể cán bộ, nhân viên nhằm hạn chế rủi ro tấn công mạng, lộ lọt dữ liệu xuất phát từ sự thiếu hiểu biết, thiếu tuân thủ chính sách và tính chủ quan của người dùng.

- Định kỳ triển khai công tác quản lý rủi ro¹⁰ an ninh mạng nhằm tăng cường khả năng phòng thủ chủ động, thực hiện xác định, đánh giá và triển khai các biện pháp giảm thiểu rủi ro, đồng thời chuẩn bị phương án¹¹ ứng phó khi rủi ro xảy ra để hạn chế tối đa hậu quả. Chú trọng công tác kiểm tra tuân thủ và cập nhật định kỳ quy định, quy trình hoạt động của bộ phận kỹ thuật, chính sách, quy chế bảo đảm an ninh mạng, quy

⁶ Căn cứ Điểm c khoản 1 Điều 40. Trách nhiệm của chủ quản hệ thống thông tin trong bảo vệ an ninh mạng tại Luật An ninh mạng năm 2025. Trung tâm giám sát an ninh mạng tỉnh (SOC) Khánh Hòa là một trong các dự án chuyển đổi số phục vụ công tác quản lý, giám sát ATTT mạng trên toàn tỉnh đang được triển khai trong năm 2026.

⁷ Tối thiểu bao gồm: (1) Các quy định, quy trình quản lý, vận hành, bảo vệ hệ thống thông tin; (2) Quy chế đảm bảo an ninh mạng cho hệ thống thông tin, đảm bảo tuân thủ quy định của pháp luật về an ninh mạng đáp ứng các yêu cầu tại mục 4 của tiêu chuẩn TCVN 14423:2025 đối với hệ thống thông tin của cơ quan nhà nước.

⁸ Thiết lập, tuân thủ và duy trì quy trình, sử dụng công cụ để phân quyền và quản lý quyền truy cập của tài khoản người dùng bao gồm: tài khoản quản trị, tài khoản tác nghiệp (tài khoản của người dùng cuối tác nghiệp), tài khoản kỹ thuật (tài khoản dùng để kết nối giữa các hệ thống kỹ thuật), tài khoản dịch vụ (tài khoản cấp cho người thụ hưởng dịch vụ) trên các tài sản phần cứng và phần mềm; xây dựng và thực thi quy trình tạo, gán, quản lý, thu hồi đặc quyền và quyền truy cập đối với các tài khoản người dùng cho tài sản phần cứng và phần mềm. Quyền truy cập của tài khoản quản trị, tài khoản tác nghiệp, tài khoản kỹ thuật, tài khoản dịch vụ phải nhất quán dựa trên vai trò và các yêu cầu cụ thể, đảm bảo người dùng chỉ có quyền truy cập vào dữ liệu, tài sản phù hợp; tổ chức ghi nhật ký và giám sát tài khoản người dùng.

⁹ Các loại dữ liệu cần được xác định, bảo vệ sao lưu và khôi phục cơ bản sau: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu, dữ liệu, thông tin nghiệp vụ; xác định tần suất sao lưu và khôi phục tương ứng với từng loại dữ liệu đã định nghĩa; xác định phương pháp sao lưu và khôi phục tương ứng với từng loại dữ liệu đã định nghĩa; quản lý vùng lưu trữ dữ liệu sao lưu, đảm bảo tính toàn vẹn của dữ liệu và khôi phục dữ liệu một cách nhanh, hiệu quả. Định kỳ thực hiện khôi phục dữ liệu đã sao lưu dựa trên mức độ nhạy cảm và tầm quan trọng của dữ liệu nhằm kiểm tra khả năng khôi phục của bản sao lưu. Tùy vào mức độ quan trọng của dữ liệu đã được xác định, cơ quan, đơn vị xây dựng giải pháp thực hiện hoặc triển khai các biện pháp, hướng dẫn từ Trung ương để đáp ứng các yêu cầu tại tiêu chuẩn quốc gia “TCVN 14423:2025” quy định cụ thể từ Mục 5.4.2.4 đến 5.4.2.9.

¹⁰ Tùy thuộc vào cấp độ quan trọng của hệ thống thông tin (Cấp độ 1 đến Cấp độ 5), tần suất thực hiện sẽ có sự khác biệt, nhưng thông thường tuân theo các mốc sau: Định kỳ hàng năm (tối thiểu 01 lần/năm), định kỳ 6 tháng/3 tháng một lần, đột xuất (khi có biến động lớn).

¹¹ Tham khảo Phương án số 1921/PA-CQTTTB ngày 29/12/2025 của Công an tỉnh - Cơ quan Thường trực Tiểu ban An ninh mạng về việc đảm an ninh, an toàn thông tin và ứng cứu sự cố an ninh mạng, thực hiện hiệu quả các giải pháp bảo đảm an ninh mạng, an toàn thông tin cho các cơ sở dữ liệu, hệ thống thông tin phục vụ chuyển đổi số trong toàn hệ thống chính trị; Chương trình hành động số 17-CTr/TU, ngày 02/4/2026 về thực hiện Chỉ thị số 57-CT/TW của Ban Bí thư về tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị.

trình quản trị, vận hành hệ thống, quản lý thay đổi, ứng cứu sự cố; đảm bảo các quy trình, quy định, chính sách được ban hành sát với thực tiễn, có hiệu quả, không mang tính thủ tục, hành chính.

- Nâng cao hiệu quả công tác bảo đảm an ninh dữ liệu, an ninh thông tin, bảo vệ thông tin thuộc phạm vi bí mật nhà nước thông qua việc tuân thủ tuyệt đối quy định của pháp luật¹², trong đó tập trung áp dụng các biện pháp cách ly vật lý, mã hóa cơ yếu và kiểm soát chặt chẽ quyền truy cập, tăng cường quản lý định danh, xác thực người dùng ngăn chặn tình trạng thu thập, khai thác và sử dụng trái phép thông tin công dân.

- Thực hiện nhiệm vụ số 15, 16 tại Mục I, Phụ lục 3 của Kế hoạch số 2364/KH-UBND ngày 06/02/2026 của UBND tỉnh về Chuyển đổi số tỉnh Khánh Hòa năm 2026, Công an tỉnh - Cơ quan thường trực Tiểu ban An ninh mạng đã xây dựng kế hoạch¹³ kiểm tra, đánh giá an toàn thông tin mạng đối với hệ thống thông tin cấp độ 1 - 2 trong các cơ quan Đảng, cơ quan Nhà nước trên địa bàn tỉnh. Qua kiểm tra hầu hết các Trung tâm hành chính công của các UBND xã/phường tiềm ẩn nguy cơ mất an toàn an ninh thông tin, trong đó việc lưu các mật khẩu truy cập vào các hệ thống dịch vụ công trực tuyến trên các trình duyệt rất phổ biến, nguy hiểm hơn là việc lưu trữ các dữ liệu, thông tin cá nhân của người dân trên các máy tính tiếp dân, cũng như trên các máy nghiệp vụ mà không có biện pháp bảo vệ; tình trạng không chia vùng mạng, mạng wifi dùng chung cùng lớp mạng với cán bộ công chức và không đặt mật khẩu; không cấu hình bảo mật cho các thiết bị máy tính, máy in từ đó có nguy cơ các đối tượng truy cập từ xa thông qua hệ thống mạng wifi, chiếm quyền leo thang kiểm soát việc in ấn, soạn thảo tài liệu trong nội bộ các cơ quan.

- Các cơ quan, tổ chức cần triển khai cơ chế quản lý, kiểm soát kỹ thuật đối với toàn bộ vòng đời của dữ liệu, chú trọng các công tác: (1)Phân loại, xác định và gắn nhãn mức độ mật, nhạy cảm của tài liệu ngay từ khâu tạo lập, (2)Triển khai hệ thống sao lưu dự phòng tách biệt với hệ thống mạng chính, đảm bảo khả năng phục hồi dữ liệu, (3)Áp dụng các giải pháp mã hóa đối với dữ liệu trong quá trình lưu trữ và truyền đưa trên môi trường mạng, (4)Thực hiện nghiêm quy trình xóa dữ liệu an toàn hoặc tiêu hủy thiết bị lưu trữ khi không còn nhu cầu sử dụng theo quy định.

II. CẢNH BÁO NGUY CƠ VỀ AN NINH DỮ LIỆU TỪ HỆ THỐNG XÁC THỰC SINH TRẮC HỌC ĐIỆN TỬ CỦA NGÂN HÀNG

1. Trong thời gian gần đây, qua rà soát an ninh thông tin trên không gian mạng, Bộ Công an phát hiện một số đối tượng đăng tải thông tin quảng cáo, rao bán các thiết bị di động được tùy chỉnh kèm ứng dụng có tính năng vượt qua lớp xác thực sinh trắc (*khuôn mặt*) của ứng dụng ngân hàng điện tử. Được biết đến nay, thiết bị có khả năng vượt qua hoặc hỗ trợ vượt qua tính xác thực trên ứng dụng điện tử (*dịch vụ internet banking, mobile banking...*) của một số ngân hàng tại Việt Nam và số lượng ngân hàng bị tác động có thể tiếp tục gia tăng trong thời gian tới. Các đối tượng thường yêu cầu

¹² Luật An ninh mạng 2025, Luật Bảo vệ bí mật nhà nước 2025, Luật Bảo vệ dữ liệu 2025, Luật Dữ liệu 2024, Luật Bảo vệ dữ liệu cá nhân và các văn bản hướng dẫn dưới luật đi kèm.

¹³ Tiến độ thực hiện Kế hoạch Pentest 159 đơn vị trên địa bàn tỉnh: Từ ngày 17/4 – 17/6/2026, Tổ Công tác đã đạt tiến độ với 72/159 đơn vị được kiểm tra, đánh giá giai đoạn 2, đạt tỉ lệ 45% Kế hoạch đề ra; tích lũy kế toán dự án, hiện đã có 54/159 đơn vị hoàn thành việc đánh giá an ninh mạng, đạt tỉ lệ 34%.

người mua thực hiện phương thức thanh toán bằng tiền điện tử trên các sàn giao dịch tài sản mã hóa quốc tế.

2. Việc xuất hiện thiết bị, phần mềm có khả năng vượt qua “chốt chặn” sinh trắc học khuôn mặt ứng dụng ngân hàng điện tử nhiều khả năng do các nhóm nghiên cứu kỹ thuật công nghệ nước ngoài sản xuất; gây rủi ro, nguy hại đến an ninh hệ thống ngân hàng và an toàn của người dân khi sử dụng dịch vụ. Đây là điều kiện thuận lợi để các nhóm tội phạm mạng tiếp cận công nghệ giả rẻ phục vụ cho hoạt động phạm pháp, đặc biệt đối với hoạt động lừa đảo trực tuyến, rửa tiền, sử dụng tài khoản cho thuê/mượn thực hiện hành vi trái pháp luật. Vì vậy, các cơ quan, đơn vị cần thông báo đến các cán bộ, công chức, viên chức, người lao động biết để kịp thời phối hợp với Công an tỉnh thực hiện: (1) Bảo quản, giữ gìn thông tin, tài liệu cá nhân (***hình ảnh riêng tư, thông tin tài khoản ngân hàng, tài khoản trên các website-internet banking và ứng dụng mạng xã hội***) đang lưu trữ, đặc biệt là lưu trữ trên điện thoại di động và máy tính cá nhân và các thiết bị điện tử thường xuyên kết nối Internet công cộng; hạn chế việc đăng, tải hình ảnh cá nhân lên các ứng dụng mạng xã hội (Facebook, Instagram, Zalo...), ***đặc biệt là đối với các hình chụp chính diện gương mặt ở chế độ rõ, sắc nét (x1) và được chụp với khoảng cách từ mặt đến camera từ 17cm-25cm***); (2) Đấu tranh, ngăn chặn và xử lý nghiêm các hành vi vi phạm pháp luật như: mua bán, sử dụng thiết bị, phần mềm/ứng dụng có tính năng nêu trên để trục lợi, gây ảnh hưởng đến lợi ích hợp pháp của cá nhân, tổ chức. Đồng thời, tổ chức tuyên truyền đến quần chúng nhân dân về phương thức, thủ đoạn này để phòng tránh; tăng cường ý thức tự bảo vệ thông tin cá nhân (đặc điểm sinh trắc học) khi thực hiện các giao dịch điện tử, thanh toán điện tử và hoạt động trên không gian mạng.

* Quá trình rà soát, thực hiện các biện pháp tăng cường bảo đảm an ninh mạng cho hệ thống thông tin quan trọng, bảo mật thông tin và an ninh dữ liệu nếu gặp khó khăn, vướng mắc, đề nghị quý cơ quan, đơn vị trao đổi về Văn phòng Tiểu ban An ninh mạng tỉnh Khánh Hòa (Đầu mối liên hệ: Đồng chí Thiếu tá Phan Võ Minh Ngọc, SĐT: 091.468.5712) để được hướng dẫn, hỗ trợ.

Đề nghị các sở, ban, ngành và UBND các cấp quan tâm, phối hợp thực hiện. 

Nơi nhận:

- Như trên;
- UBND tỉnh (báo cáo);
- Đồng chí Giám đốc CAT (báo cáo);
- Lưu: VT, ANM.



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