BỘ CÔNG AN
CÔNG AN TỈNH KHÁNH HÒA

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

Số: 4319 /CAT-ANM
V/v thông báo kế hoạch 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 Khánh Hòa

Khánh Hòa, ngày 15 tháng 04 năm 2026

Kính gửi:

- Văn phòng Tỉnh ủy;
- Văn phòng UBND tỉnh;
- Cơ quan khối Đảng: *Các cơ quan tham mưu, giúp việc Tỉnh ủy; các Đảng ủy trực thuộc Tỉnh ủy; các Đảng ủy xã, phường, đặc khu;*
- Cơ quan khối Nhà nước: *Các Sở, ban, ngành; các đơn vị sự nghiệp trực thuộc UBND tỉnh; UBND xã, phường, đặc khu;*

(Theo danh sách tại Phụ lục 03)

Triển khai thực hiện các nhiệm vụ được giao tại Kế hoạch số 2364/KH-UBND ngày 06/02/2026 của UBND tỉnh về Chuyển đổi số tỉnh Khánh Hòa năm 2026 (nhiệm vụ 15, 16 mục I Phụ lục 03);

Công an tỉnh - Cơ quan thường trực Tiểu ban An ninh mạng thông báo kế hoạch kiểm tra, đánh giá an toàn thông tin mạng đối với hệ thống thông tin cấp độ 1-2 của các cơ quan Đảng và cơ quan Nhà nước trên địa bàn tỉnh, cụ thể như sau:

I. PHẠM VI TRIỂN KHAI

Triển khai kiểm tra, đánh giá an toàn thông tin mạng đối với các hệ thống thông tin cấp độ 1, 2 của các cơ quan, đơn vị trên địa bàn tỉnh, gồm:

- 73 đơn vị khối Đảng (các cơ quan tham mưu, giúp việc Tỉnh ủy; các Đảng ủy trực thuộc Tỉnh ủy; các Đảng ủy xã, phường);
- 86 cơ quan nhà nước (các Sở, ban, ngành; các đơn vị sự nghiệp trực thuộc UBND tỉnh; UBND các xã, phường).

II. KẾ HOẠCH KIỂM TRA, ĐÁNH GIÁ AN TOÀN THÔNG TIN

1. Nội dung kiểm tra, đánh giá ATTT

1.1 Kiểm tra, đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin theo phương án bảo đảm an toàn thông tin được phê duyệt (quy định tại điểm b khoản 1 Điều 11 và điểm c, d, đ khoản 2 Điều 12 Thông tư số 12/2022/TT-BTTTT)

a) Đánh giá việc thiết kế hệ thống theo phương án bảo đảm an toàn thông tin được phê duyệt.

b) Đánh giá việc thiết lập, cấu hình hệ thống theo phương án bảo đảm an toàn thông tin được phê duyệt.

c) Kiểm tra việc cấu hình, tăng cường bảo mật cho thiết bị hệ thống, hệ điều hành, ứng dụng, cơ sở dữ liệu và các thành phần khác liên quan trong hệ thống theo hướng dẫn của các cơ quan chức năng.

1.2. Kiểm tra, đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thông tin (quy định tại điểm c khoản 1 Điều 11 và điểm a, b, c khoản 3 Điều 12 c)

a) Dò quét, phát hiện mã độc, lỗ hổng, điểm yếu của hệ thống, thử nghiệm tấn công xâm nhập đối với các thiết bị hệ thống, hệ điều hành, ứng dụng, cơ sở dữ liệu và các thành phần khác liên quan trong hệ thống;

b) Đánh giá an toàn mã nguồn đối với phần mềm nội bộ;

c) Đưa ra phương án và kế hoạch xử lý lỗ hổng, điểm yếu và phương án cấu hình, tăng cường bảo mật đối với các nội dung kiểm tra được đánh giá là chưa đạt.

2. Kế hoạch triển khai thực hiện

2.1. Tập huấn, hướng dẫn

a) Thành phần tham gia:

- Cơ quan, đơn vị được kiểm tra: Đại diện lãnh đạo bộ phận phụ trách công tác an toàn thông tin; cán bộ đầu mối kỹ thuật CNTT; cán bộ phụ trách hồ sơ cấp độ ATTT; cán bộ trực tiếp tham gia vận hành hệ thống mạng nội bộ cơ quan, các hệ thống thông tin.

- Công an tỉnh: Cán bộ Phòng An ninh mạng và Phòng chống tội phạm sử dụng công nghệ cao và các đơn vị liên quan.

- Đơn vị tư vấn: Tổ trưởng kỹ thuật, chuyên gia kỹ thuật, nhân sự chuyên môn, quản lý dự án.

b) Hình thức thực hiện: Trực tuyến.

c) Nội dung tập huấn:

- Hướng dẫn cung cấp thông tin, số liệu hiện trạng.

- Hướng dẫn xây dựng hồ sơ cấp độ an toàn thông tin.

- Phổ biến nội dung kế hoạch thực hiện kiểm tra an toàn thông tin; các công việc phối hợp, thực hiện trước, trong và sau đợt kiểm tra tại đơn vị.

- Các biên bản, văn bản xác nhận liên quan.

d) Thời gian thực hiện: 01 buổi/đợt; dự kiến 03 đợt theo tiến độ của từng giai đoạn *(Công an tỉnh sẽ thông báo lịch đào tạo cụ thể trên các nhóm)*.

2.2. Giai đoạn 01: Triển khai diện hẹp và đánh giá

a) Mục tiêu: Triển khai tại 03 đơn vị trọng điểm vận hành thực tế để kịp thời nhận diện các vướng mắc phát sinh trong quá trình phối hợp thực hiện; tạo cơ sở thực tiễn hoàn thiện các bước, quy trình triển khai.

b) Danh sách **03** cơ quan, đơn vị kiểm tra:

- Đảng ủy phường Nha Trang.

- Đảng ủy xã Thuận Nam.

- Báo và Phát thanh, Truyền hình Khánh Hòa.

c) Thành phần tham gia:

- Cơ quan, đơn vị được kiểm tra: Đại diện lãnh đạo bộ phận phụ trách công tác an toàn thông tin; cán bộ đầu mối kỹ thuật CNTT; cán bộ phụ trách hồ sơ cấp độ ATTT; cán bộ trực tiếp tham gia vận hành hệ thống mạng nội bộ cơ quan, các hệ thống thông tin.

- Công an tỉnh: Cán bộ Phòng An ninh mạng và Phòng chống tội phạm sử dụng công nghệ cao và các đơn vị liên quan.

- Đơn vị tư vấn: Tổ trưởng kỹ thuật, chuyên gia kỹ thuật, nhân sự chuyên môn, quản lý dự án.

- Thành lập các tổ công tác tham gia triển khai: Dự kiến 05 tổ, mỗi tổ gồm các thành phần: Đơn vị tư vấn *(Tổ trưởng kỹ thuật, Chuyên gia kỹ thuật, Nhân sự chuyên môn, Quản lý dự án)*, Công an tỉnh.

d) Hình thức thực hiện: Trực tiếp tại trụ sở cơ quan, đơn vị (bao gồm trụ sở chính và các trụ sở thành phần).

e) Nội dung, phương án thực hiện: *Chi tiết* ***Phụ lục 01 và 02.***

g) Thời gian thực hiện: Từ ngày 16/4/2026 - 24/4/2026, *xem lịch chi tiết tại* ***Phụ lục 01.***

2.3. Giai đoạn 02: Triển khai mở rộng toàn tỉnh

a) Mục tiêu: Trên cơ sở quy trình triển khai đã được tối ưu hóa từ Giai đoạn 1 để triển cho các cơ quan, đơn vị còn lại thuộc phạm vi nhiệm vụ.

b) Danh sách **156** cơ quan, đơn vị kiểm tra: *Chi tiết* ***Phụ lục 03.***

- 70 đơn vị khối Đảng còn lại (các cơ quan tham mưu, giúp việc Tỉnh ủy; các Đảng ủy trực thuộc Tỉnh ủy; các Đảng ủy xã, phường).

- 86 cơ quan nhà nước (các Sở, ban, ngành; các đơn vị sự nghiệp trực thuộc UBND tỉnh; UBND các xã, phường).

c) Thành phần tham gia:

- Cơ quan, đơn vị được kiểm tra: Đại diện lãnh đạo bộ phận phụ trách công tác an toàn thông tin; cán bộ đầu mối kỹ thuật CNTT; cán bộ phụ trách hồ sơ cấp độ ATTT; cán bộ trực tiếp tham gia vận hành hệ thống mạng nội bộ cơ quan, các hệ thống thông tin.

- Công an tỉnh: Cán bộ Phòng An ninh mạng và Phòng chống tội phạm sử dụng công nghệ cao và các đơn vị liên quan.

- Đơn vị tư vấn: Tổ trưởng kỹ thuật, chuyên gia kỹ thuật, nhân sự chuyên môn, quản lý dự án.

- Thành lập các tổ công tác tham gia triển khai: Dự kiến 05 tổ, mỗi tổ gồm các thành phần: Đơn vị tư vấn *(Tổ trưởng kỹ thuật, Chuyên gia kỹ thuật, Nhân sự chuyên môn, Quản lý dự án)*, Công an tỉnh.

d) Hình thức thực hiện: Trực tiếp tại trụ sở cơ quan, đơn vị (bao gồm trụ sở chính và các trụ sở thành phần).

e) Nội dung, phương án thực hiện: *Chi tiết* ***Phụ lục 01 và 02.***

g) Thời gian thực hiện: Dự kiến từ ngày 11/5/2026 - 15/6/2026.

Ghi chú: Đối với Giai đoạn 02, Công an tỉnh sẽ có văn bản thông báo chi tiết lịch kiểm tra, đánh giá cụ thể tại từng cơ quan, đơn vị, địa phương theo các đợt công tác.

III. CÔNG TÁC CHUẨN BỊ

1. Yêu cầu đối với các cơ quan, đơn vị được kiểm tra:

a) Cơ quan, đơn vị, địa phương tại Phụ lục 01 và 03 cử và cung cấp danh sách lãnh đạo bộ phận phụ trách công tác ATTT; cán bộ đầu mối kỹ thuật CNTT; cán bộ phụ trách hồ sơ cấp độ ATTT; cán bộ trực tiếp tham gia vận hành hệ thống mạng nội bộ cơ quan, các hệ thống thông tin *(bao gồm: Họ tên, chức vụ, cơ quan/đơn vị, số điện thoại Zalo)* về Công an tỉnh **trước ngày 15/4/2026** theo biểu mẫu tại địa chỉ mã QR sau:

b) Các cán bộ đầu mối tại điểm a nêu trên có trách nhiệm:

(1) Tham gia nhóm trao đổi do Công an tỉnh lập để kịp thời thông tin các nội dung liên quan trước/trong và sau quá trình thực hiện công tác kiểm tra, đánh giá ATTT tại địa chỉ mã QR sau:

(2) Cung cấp đầy đủ thông tin hiện trạng hạ tầng CNTT, bảo đảm ATTT theo các biểu mẫu; (3) Cung cấp dự thảo hồ sơ cấp độ ATTT và xây dựng hoàn thiện hồ sơ cấp độ theo hướng dẫn; (4) Tham gia đầy đủ các lớp tập huấn, hướng dẫn theo triệu tập tại Mục 2.1 nêu trên.

2. Thông tin liên hệ:

Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh, số điện thoại: *Đ/c Nguyễn Thị Thơm - 0988.810.685; Đ/c Đoàn Văn Tài - 0899.377.968.*

Công an tỉnh đề nghị cơ quan, đơn vị, địa phương quan tâm, thực hiện./.

Nơi nhận:
- Như trên (VBĐT);
- Đ/c Giám đốc CAT (VBĐT, báo cáo);
- Đ/c Bí thư Tỉnh ủy, Trưởng Tiểu ban ANM; các đ/c Phó Trưởng Tiểu ban ANM (VBĐT, báo cáo);
- VP Tỉnh ủy, VP UBND tỉnh (VBĐT);
- Lưu: VT, ANM (NT).

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Đại tá Nguyễn Đình Thuận Hải

Phụ lục 01
KẾ HOẠCH TRIỂN KHAI THEO GIAI ĐOẠN
(Kèm theo Công văn số /CAT-ANM ngày …./ /2026 của Công an tỉnh)

1. Giai đoạn 01: Triển khai diện hẹp và đánh giá

- **Thời gian:** Từ ngày 16/4/2026 - 24/4/2026.

STT	Đơn vị	Tổ công tác	Thời gian dự kiến	Địa điểm
1	Đảng ủy phường Nha Trang	TỔ I	16 - 17/4/2026	Trụ sở đơn vị
2	Báo và Phát thanh, Truyền hình Khánh Hòa	TỔ I + TỔ II	20 - 22/4/2026	Trụ sở đơn vị
3	Đảng ủy xã Thuận Nam	TỔ II	20 - 22/4/2026	Trụ sở đơn vị

2. Giai đoạn 02: Triển khai mở rộng toàn tỉnh

- **Thời gian:** Dự kiến từ ngày 11/5/2026 - 15/6/2026.

STT	Khu vực	Tổ công tác	Thời gian dự kiến	Địa điểm
1	KHU VỰC I	TỔ I	11/5 – 17/6	Trụ sở đơn vị
2	KHU VỰC II	TỔ II + TỔ III + TỔ IV + TỔ V	4/5 – 31/5	Trụ sở đơn vị
3	KHU VỰC III	TỔ I	11/6 – 26/6	Trụ sở đơn vị
4	KHU VỰC IV	TỔ II + TỔ III + TỔ IV + TỔ V	23/5 – 17/6	Trụ sở đơn vị

Lưu ý đối với Giai đoạn 02:

- *Công an tỉnh sẽ có văn bản thông báo lịch kiểm tra, đánh giá cụ thể tại từng cơ quan, đơn vị, địa phương.*
- *Có thể điều chỉnh lịch theo tình hình thực tế.*
- *Danh sách các cơ quan, đơn vị tại Phụ lục 03.*

Phụ lục 02
NỘI DUNG, PHƯƠNG ÁN THỰC HIỆN KIỂM TRA
(Kèm theo Công văn số /CAT-ANM ngày …./ /2026 của Công an tỉnh)

1. Kiểm tra, đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin theo phương án bảo đảm an toàn thông tin được phê duyệt

1.1. Đánh giá việc thiết kế hệ thống theo phương án bảo đảm an toàn thông tin được phê duyệt

Đối với HTTT cấp độ 1

Thực hiện kiểm tra, đánh giá thiết kế hệ thống theo tiêu chí "Đạt" hoặc "Không đạt" và đưa ra khuyến nghị khắc phục với các nội dung như sau:

a) Thiết kế các vùng mạng trong hệ thống theo chức năng, các vùng mạng tối thiểu bao gồm:

+ Vùng mạng nội bộ

+ Vùng mạng biên

+ Vùng DMZ

b) Có phương án thiết kế bảo đảm các yêu cầu sau:

+ Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn sử dụng mạng riêng ảo hoặc phương án tương đương;

+ Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập, sử dụng sản phẩm Tường lửa có tích hợp chức năng phòng, chống xâm nhập hoặc phương án tương đương;

+ Có phương án phòng chống mã độc cho máy chủ và máy trạm sử dụng sản phẩm Phòng chống mã độc hoặc phương án tương đương.

Đối với HTTT cấp độ 2

Thực hiện kiểm tra, đánh giá thiết kế hệ thống theo tiêu chí "Đạt" hoặc "Không đạt" và đưa ra khuyến nghị khắc phục với các nội dung như sau:

a) Thiết kế các vùng mạng trong hệ thống theo chức năng, các vùng mạng tối thiểu bao gồm:

+ Vùng mạng nội bộ;

+ Vùng mạng biên;

+ Vùng DMZ;

+ Vùng máy chủ nội bộ;

+ Vùng mạng không dây (nếu có) tách riêng, độc lập với các vùng mạng

b) Có phương án thiết kế bảo đảm các yêu cầu sau:

+ Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn sử dụng mạng riêng ảo hoặc phương án tương đương;

+ Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập, sử dụng sản phẩm Tường lửa có tích hợp chức năng phòng, chống xâm nhập hoặc phương án tương đương;

+ Có phương án phòng chống mã độc cho máy chủ và máy trạm sử dụng sản phẩm Phòng chống mã độc hoặc phương án tương đương;

+ Có phương án phòng chống tấn công mạng cho ứng dụng web; sử dụng sản phẩm Tường lửa ứng dụng web đối với hệ thống thông tin theo quy định tại khoản 2 Điều 8 Nghị định 85/2016/NĐ-CP;

+ Có phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử đối với hệ thống thư điện tử;

+ Có phương án dự phòng cho các thiết bị mạng chính, bao gồm thiết bị chuyển mạch trung tâm hoặc tương đương, thiết bị tường lửa trung tâm.

1.2. Đánh giá việc thiết lập, cấu hình hệ thống theo phương án bảo đảm an toàn thông tin được phê duyệt; Kiểm tra việc cấu hình, tăng cường bảo mật cho thiết bị hệ thống, hệ điều hành, ứng dụng, cơ sở dữ liệu và các thành phần khác liên quan trọng hệ thống.

Đối với HTTT cấp độ 1:

Danh sách kiểm tra, đánh giá an toàn thông tin theo tiêu chí "Đạt" hoặc "Không đạt" và đưa ra khuyến nghị khắc phục với các nội dung như sau:

STT	Yêu cầu	TCVN 11930:2017 [1]
1.1	**Bảo đảm an toàn mạng**	**Mục 5.2.1 – Bảo đảm an toàn mạng**
1.1.1	Kiểm soát truy cập từ bên ngoài mạng	Mục 5.2.1.2 – Kiểm soát truy cập từ bên ngoài mạng a. Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập thông tin nội bộ hoặc quản trị hệ thống từ các mạng bên ngoài và mạng Internet; b. Kiểm soát truy cập từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể; chặn tất cả truy cập tới các dịch vụ, ứng dụng mà hệ thống không cung cấp hoặc không cho phép truy cập từ bên ngoài.
1.1.2	Nhật kí hệ thống	Mục 5.2.1.3 – Nhật kí hệ thống

[1] *Tiêu chuẩn quốc gia TCVN 11930:2017 về "Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ"*

STT	Yêu cầu	TCVN 11930:2017 [1]
		Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên các thiết bị mạng chính.
1.1.3	Phòng chống xâm nhập	Mục 5.2.1.4 – Phòng chống xâm nhập a. Có phương án phòng chống xâm nhập để bảo vệ vùng DMZ; b. Định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng (Signatures).
1.1.4	Bảo vệ thiết bị hệ thống	Mục 5.2.1.5 – Bảo vệ thiết bị hệ thống a. Cấu hình chức năng xác thực trên các thiết bị hệ thống (nếu hỗ trợ) để xác thực người dùng khi quản trị thiết bị trực tiếp hoặc từ xa; b. Thiết lập cấu hình chỉ cho phép sử dụng các kết nối mạng an toàn (nếu hỗ trợ) khi truy cập, quản trị thiết bị từ xa.
1.2	**Bảo đảm an toàn máy chủ**	**Mục 5.2.2 – Bảo đảm an toàn máy chủ**
1.2.1	Xác thực	Mục 5.2.2.1 – Xác thực a. Thiết lập chính sách xác thực trên máy chủ để xác thực người dùng khi truy cập, quản lý và sử dụng máy chủ; b. Thay đổi các tài khoản mặc định trên hệ thống hoặc vô hiệu hóa (nếu không sử dụng); c. Thiết lập cấu hình máy chủ để đảm bảo an toàn mật khẩu người sử dụng, bao gồm các yêu cầu sau: - Yêu cầu thay đổi mật khẩu mặc định; - Thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự.
1.2.2	Kiểm soát truy cập	Mục 5.2.2.2 – Kiểm soát truy cập Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa.
1.2.3	Nhật ký hệ thống	Mục 5.2.2.3 – Nhật ký hệ thống

STT	Yêu cầu	TCVN 11930:2017 [1]
		a. Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau; - Thông tin kết nối mạng tới máy chủ (Firewall log); - Thông tin đăng nhập vào máy chủ. b. Đồng bộ thời gian giữa máy chủ với máy chủ thời gian.
1.2.4	Phòng chống xâm nhập	Mục 5.2.2.4 – Phòng chống xâm nhập a. Loại bỏ các tài khoản không sử dụng, các tài khoản không còn hợp lệ trên máy chủ; b. Sử dụng tường lửa của hệ điều hành và hệ thống để cấm các truy cập trái phép tới máy chủ.
1.2.5	Phòng chống phần mềm độc hại	Mục 5.2.2.5 – Phòng chống phần mềm độc hại Cài đặt phần mềm phòng chống mã độc (hoặc có phương án khác tương đương) và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm.
1.3	**Bảo đảm an toàn ứng dụng**	**Mục 5.2.3 – Bảo đảm an toàn ứng dụng**
1.3.1	Xác thực	Mục 5.2.3.1 – Xác thực a. Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng; b. Lưu trữ có mã hóa thông tin xác thực hệ thống; c. Thiết lập cấu hình ứng dụng để đảm bảo an toàn mật khẩu người sử dụng, bao gồm các yêu cầu sau: - Yêu cầu thay đổi mật khẩu mặc định; - Thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự.
1.3.2	Kiểm soát truy cập	Mục 5.2.3.2 – Kiểm soát truy cập a. Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị ứng dụng từ xa;

STT	Yêu cầu	TCVN 11930:2017 [1]
		b. Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng.
1.3.3	Nhật kí hệ thống	Mục 5.2.3.3 – Nhật kí hệ thống Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau: - Thông tin truy cập ứng dụng; - Thông tin đăng nhập khi quản trị ứng dụng.
1.4	**Bảo đảm an toàn dữ liệu**	**Mục 5.2.4 – Bảo đảm an toàn dữ liệu**
1.4.1	Sao lưu dự phòng	Mục 5.2.4.1 – Sao lưu dự phòng Thực hiện sao lưu dự phòng các thông tin, dữ liệu quan trọng trên hệ thống.

Đối với HTTT cấp độ 2:

Danh sách kiểm tra, đánh giá an toàn thông tin theo tiêu chí "Đạt" hoặc "Không đạt" và đưa ra khuyến nghị khắc phục với các nội dung như sau:

STT	Yêu cầu	TCVN 11930:2017
1.1	**Bảo đảm an toàn mạng**	**Mục 6.2.1 – Bảo đảm an toàn mạng**
1.1.1	Kiểm soát truy cập từ bên ngoài mạng	Mục 6.2.1.2 – Kiểm soát truy cập từ bên ngoài mạng a. Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập thông tin nội bộ hoặc quản trị hệ thống từ các mạng bên ngoài và mạng Internet; b. Kiểm soát truy cập từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể; chặn tất cả truy cập tới các dịch vụ, ứng dụng mà hệ thống không cung cấp hoặc không cho phép truy cập từ bên ngoài; c. Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi hệ thống không nhận được yêu cầu từ người dùng.
1.1.2	Kiểm soát truy cập từ bên trong mạng	Mục 6.2.1.3 – Kiểm soát truy cập từ bên trong mạng

STT	Yêu cầu	TCVN 11930:2017
		Chỉ cho phép truy cập các ứng dụng, dịch vụ bên ngoài theo yêu cầu nghiệp vụ, chặn các dịch vụ khác không phục vụ hoạt động nghiệp vụ theo chính sách của tổ chức.
1.1.3	Nhật kí hệ thống	Mục 6.2.1.4 – Nhật ký hệ thống a. Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên các thiết bị hệ thống (nếu có); b. Sử dụng máy chủ thời gian để đồng bộ thời gian giữa các thiết bị mạng, thiết bị đầu cuối và các thành phần khác trong hệ thống tham gia hoạt động giám sát.
1.1.4	Phòng chống xâm nhập	Mục 6.2.1.5 – Phòng chống xâm nhập a. Có phương án phòng chống xâm nhập để bảo vệ vùng DMZ và vùng máy chủ nội bộ; b. Định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng (Signatures).
1.1.5	Bảo vệ thiết bị hệ thống	Mục 6.2.1.6 – Bảo vệ thiết bị hệ thống a. Cấu hình chức năng xác thực trên các thiết bị hệ thống (nếu hỗ trợ) để xác thực người dùng khi quản trị thiết bị trực tiếp hoặc từ xa; b. Thiết lập cấu hình chỉ cho phép sử dụng các kết nối mạng an toàn (nếu hỗ trợ) khi truy cập, quản trị thiết bị từ xa; c. Cấu hình thiết bị (nếu hỗ trợ) chỉ cho phép hạn chế các địa chỉ mạng có thể kết nối, quản trị thiết bị từ xa.
1.2	**Bảo đảm an toàn máy chủ**	**Mục 6.2.2 – Bảo đảm an toàn máy chủ**
1.2.1	Xác thực	Mục 6.2.2.1 – Xác thực a. Thiết lập chính sách xác thực trên máy chủ để xác thực người dùng khi truy cập, quản lý và sử dụng máy chủ; b. Thay đổi các tài khoản mặc định trên hệ thống hoặc vô hiệu hóa (nếu không sử dụng); c. Thiết lập cấu hình máy chủ để đảm bảo an toàn mật khẩu người sử dụng, bao gồm các yêu cầu sau: - Yêu cầu thay đổi mật khẩu

STT	Yêu cầu	TCVN 11930:2017
		- mặc định; - Thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự; - Thiết lập thời gian yêu cầu thay đổi mật khẩu; - Thiết lập thời gian mật khẩu hợp lệ.
1.2.2	Kiểm soát truy cập	Mục 6.2.2.2 – Kiểm soát truy cập a. Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa; b. Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi máy chủ không nhận được yêu cầu từ người dùng.
1.2.3	Nhật ký hệ thống	Mục 6.2.2.3 – Nhật ký hệ thống a. Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau: - Thông tin kết nối mạng tới máy chủ (Firewall log); - Thông tin đăng nhập vào máy chủ; - Lỗi phát sinh trong quá trình hoạt động; - Thông tin thay đổi cấu hình máy chủ; - Thông tin truy cập dữ liệu và dịch vụ quan trọng trên máy chủ (nếu có). b. Đồng bộ thời gian giữa máy chủ với máy chủ thời gian; c. Lưu nhật ký hệ thống trong khoảng thời gian tối thiểu là 01 tháng.
1.2.4	Phòng chống xâm nhập	Mục 6.2.2.4 – Phòng chống xâm nhập a. Loại bỏ các tài khoản không sử dụng, các tài khoản không còn hợp lệ trên máy chủ; b. Sử dụng tường lửa của hệ điều hành và hệ thống để cấm các truy cập trái phép tới máy chủ; c. Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ hệ thống không sử dụng; d. Có phương án cập nhật bản vá, xử lý điểm yếu an toàn thông tin cho hệ điều hành và các dịch vụ hệ thống trên máy chủ.

STT	Yêu cầu	TCVN 11930:2017
1.2.5	Phòng chống phần mềm độc hại	Mục 6.2.2.5 – Phòng chống phần mềm độc hại a. Cài đặt phần mềm phòng chống mã độc (hoặc có phương án khác tương đương) và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm; b. Có phương án kiểm tra, dò quét, xử lý phần mềm độc hại cho các phần mềm trước khi cài đặt.
1.2.6	Xử lý máy chủ khi chuyển giao	Mục 6.2.2.6 – Xử lý máy chủ khi chuyển giao Có phương án xóa sạch thông tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng.
1.3	**Bảo đảm an toàn ứng dụng**	**Mục 6.2.3 – Bảo đảm an toàn ứng dụng**
1.3.1	Xác thực	Mục 6.2.3.1 – Xác thực a. Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng; b. Lưu trữ có mã hóa thông tin xác thực hệ thống; c. Thiết lập cấu hình ứng dụng để đảm bảo an toàn mật khẩu người sử dụng, bao gồm các yêu cầu sau: - Yêu cầu thay đổi mật khẩu mặc định; - Thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự; - Thiết lập thời gian yêu cầu thay đổi mật khẩu; - Thiết lập thời gian mật khẩu hợp lệ. d. Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định.
1.3.2	Kiểm soát truy cập	Mục 6.2.3.2 – Kiểm soát truy cập a. Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị ứng dụng từ xa; b. Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng; c. Giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị ứng dụng từ xa.

STT	Yêu cầu	TCVN 11930:2017
1.3.3	Nhật kí hệ thống	Mục 6.2.3.3 – Nhật ký hệ thống a. Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau: - Thông tin truy cập ứng dụng; - Thông tin đăng nhập khi quản trị ứng dụng; - Thông tin các lỗi phát sinh trong quá trình hoạt động; - Thông tin thay đổi cấu hình ứng dụng; b. Lưu nhật ký hệ thống trong khoảng thời gian tối thiểu là 01 tháng.
1.3.4	An toàn ứng dụng và mã nguồn	Mục 6.2.3.4 – An toàn ứng dụng và mã nguồn Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý.
1.4	**Bảo đảm an toàn dữ liệu**	**Mục 6.2.4 – Bảo đảm an toàn dữ liệu**
1.4.1	Bảo mật dữ liệu	Mục 6.2.4.1 – Bảo mật dữ liệu Lưu trữ có mã hóa các thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trên hệ thống lưu trữ/phương tiện lưu trữ.
1.4.2	Sao lưu dự phòng	Mục 6.2.4.2 – Sao lưu dự phòng Thực hiện sao lưu dự phòng các thông tin, dữ liệu 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.

2. Kiểm tra, đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thông tin

2.1 Mô tả chi tiết các hạng mục của dịch vụ kiểm tra, đánh giá ATTT mạng theo hình thức kiểm tra, đánh giá Hộp xám (Greybox)

Thực hiện Kiểm tra, đánh giá ATTT mạng theo quy trình và đưa ra khuyến nghị khắc phục với các nội dung như sau:

TT	Nội dung đánh giá	Mô tả
I	**Kiểm tra đánh giá ứng dụng Web**	

TT	Nội dung đánh giá	Mô tả
1	Thu thập và khảo sát thông tin	Thực hiện tìm kiếm thông tin về ứng dụng phục vụ cho quá trình đánh giá
2	Kiểm tra quản lý cấu hình và triển khai	Việc phân tích cơ sở hạ tầng và kiến trúc của website có thể giúp xác định rất nhiều yếu tố về một ứng dụng Web.
3	Kiểm tra quản lý định danh	Xác định việc ứng dụng định danh người dùng, qua đó có thể phá vỡ tính xác thực và định danh của người dùng.
4	Kiểm tra phần xác thực	Kiểm tra cơ chế xác thực dựa trên các phân tích cơ chế hoạt động của chức năng đăng nhập trong ứng dụng Web để tìm ra các điểm yếu.
5	Kiểm tra phân quyền	Tìm hiểu chức năng cấp quyền làm việc, thử phá vỡ cơ chế quan trọng này.
6	Kiểm tra quản lý phiên	Kiểm tra xem phiên và các "security token" có được tạo ra một cách an toàn hoặc có thể đoán trước được hay không
7	Kiểm tra kiểm soát dữ liệu đầu vào	Đa phần điểm yếu trong ứng dụng Web tập trung vào khâu đánh giá đầu vào đến từ người dùng. Điểm yếu này dẫn đến hầu hết lỗ hổng trong ứng dụng Web như: "SQL Injection", "File Inclusion", "Cross-site scripting" …
8	Kiểm tra việc xử lý lỗi	Kiểm tra việc thông báo lỗi của ứng dụng có gây ra các nguy cơ mất ATTT cho hệ thống hay không.
9	Kiểm tra mật mã, mã hóa yếu	Kiểm tra các cơ chế mã hoá có thể yếu của ứng dụng.
10	Kiểm tra lỗ hổng logic nghiệp vụ	Kiểm tra việc vận hành ứng dụng có thể gây ra các lỗi mà người dùng bình thường không phát hiện ra.
II	**Kiểm tra đánh giá hệ thống Máy chủ dịch vụ, máy tính người dùng, thiết bị mạng và bảo mật**	
1	Thu thập thông tin	Thu thập thông tin của đối tượng.

TT	Nội dung đánh giá	Mô tả
2	Đánh giá xác thực	Kiểm tra cơ chế xác thực, chống các tấn công vét cạn, tấn công từ điển vào tài khoản quản trị.
3	Đánh giá phân quyền	Kiểm tra các cơ chế chống leo thang đặc quyền.
4	Đánh giá quá trình kiểm tra dữ liệu đầu vào	Kiểm tra dữ liệu nhập tại các điểm có khả năng nhận dữ liệu từ phía máy khách trên các cổng dịch vụ đang mở của máy chủ .
III	**Kiểm tra đánh giá hệ thống cơ sở dữ liệu**	
1	Thu thập thông tin Cơ sở dữ liệu	Thu thập các thông tin về máy chủ CSDL, các "Instance" của CSDL
2	Đánh giá cấu hình máy chủ cơ sở dữ liệu	Xác định cấu hình máy chủ CSDL gây mất an toàn cho hệ thống.
3	Đánh giá xác thực	Kiểm tra cơ chế xác thực, chống các tấn công vét cạn, tấn công từ điển vào tài khoản quản trị.
4	Đánh giá phân quyền	Kiểm tra các cơ chế chống leo thang đặc quyền
5	Kiểm tra các lỗ hổng CVE (Common Vulnerabilities and Exposures) liên quan tới CSDL	Thu thập thông tin CVE liên quan tới CSDL, thực hiện kiểm tra khả năng khai thác của các CVE này lên hệ thống CSDL

2.2. Đánh giá an toàn mã nguồn đối với phần mềm nội bộ theo hình thức hộp trắng (Whitebox)

Thực hiện Kiểm tra, đánh giá An toàn ứng dụng và mã nguồn [2] theo tiêu chí "Đạt" hoặc "Không đạt" và đưa ra khuyến nghị khắc phục với các nội dung như sau:

TT	An toàn ứng dụng và mã nguồn	Mô tả yêu cầu	Cấp độ của hệ thống thông tin	
			1	2
1	Có chức năng cho phép kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý.	Có chức năng thực thi việc kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý	x	x

TT	An toàn ứng dụng và mã nguồn	Mô tả yêu cầu	Cấp độ của hệ thống thông tin	
			1	2
2	Có chức năng cho phép bảo đảm không lưu trữ thông tin xác thực, thông tin bí mật trên mã nguồn ứng dụng.	Thông tin xác thực, bí mật không được đưa trực tiếp vào mã nguồn ứng dụng mà phải được thiết lập thông qua giao diện cấu hình hệ thống		x

Phụ lục 03
DANH SÁCH 159 CƠ QUAN ĐẢNG VÀ CƠ QUAN NHÀ NƯỚC
(Kèm theo Công văn số /CAT-ANM ngày …./ /2026 của Công an tỉnh)

I. Giai đoạn 01: 03 cơ quan, đơn vị

STT	Tên đơn vị	Ghi chú
1	Đảng ủy phường Nha Trang	Phường/Xã
2	Báo và Phát thanh, Truyền hình Khánh Hòa	Cơ quan Đảng cấp tỉnh
3	Đảng ủy xã Thuận Nam	Phường/Xã

II. Giai đoạn 02: 156 cơ quan, đơn vị

* Khu vực I: 37

STT	Tên đơn vị	Ghi chú
I	**CƠ QUAN ĐẢNG: 08**	
1	Ban Tổ chức Tỉnh ủy	Cơ quan Đảng cấp tỉnh
2	Ban Tuyên giáo và Dân vận Tỉnh ủy	Cơ quan Đảng cấp tỉnh
3	Ban Nội chính Tỉnh ủy	Cơ quan Đảng cấp tỉnh
4	Ủy ban Kiểm tra Tỉnh ủy	Cơ quan Đảng cấp tỉnh
5	Văn phòng Tỉnh ủy[3]	Cơ quan Đảng cấp tỉnh
6	Đảng ủy Các cơ quan Đảng tỉnh	Cơ quan Đảng cấp tỉnh
7	Đảng ủy UBND tỉnh	Cơ quan Đảng cấp tỉnh

[3] Đối với các HTTT dùng chung không cài đặt tại hạ tầng của đơn vị: Thực hiện thu thập hiện trạng, không đánh giá chuyên sâu.

STT	Tên đơn vị	Ghi chú
8	Trường Chính trị tỉnh	Cơ quan Đảng cấp tỉnh
II	**CƠ QUAN NHÀ NƯỚC: 22**	
1	Văn phòng UBND tỉnh[4]	Cơ quan Nhà nước cấp tỉnh
2	Sở Nội vụ	Cơ quan Nhà nước cấp tỉnh
3	Sở Nông nghiệp và Môi trường	Cơ quan Nhà nước cấp tỉnh
4	Sở Xây dựng	Cơ quan Nhà nước cấp tỉnh
5	Sở Tài chính	Cơ quan Nhà nước cấp tỉnh
6	Sở Khoa học và Công nghệ[5]	Cơ quan Nhà nước cấp tỉnh
7	Sở Văn hóa, Thể thao và Du lịch	Cơ quan Nhà nước cấp tỉnh
8	Sở Dân tộc và Tôn giáo	Cơ quan Nhà nước cấp tỉnh
9	Sở Giáo dục và Đào tạo	Cơ quan Nhà nước cấp tỉnh
10	Sở Công Thương	Cơ quan Nhà nước cấp tỉnh
11	Sở Y tế	Cơ quan Nhà nước cấp tỉnh
12	Sở Tư pháp	Cơ quan Nhà nước cấp tỉnh
13	Thanh tra tỉnh	Cơ quan Nhà nước cấp tỉnh
14	Ban Quản lý dự án phát triển tỉnh	Đơn vị sự nghiệp

[4] Bao gồm 02 Trung tâm Phục vụ hành chính công cấp tỉnh.
[5] Đối với Trung tâm dữ liêu tỉnh: Thực hiện thu thập hiện trạng, không đánh giá chuyên sâu.

STT	Tên đơn vị	Ghi chú
15	Ban Quản lý khu kinh tế và khu công nghiệp tỉnh	Đơn vị sự nghiệp
16	Ban Quản lý dự án đầu tư xây dựng các công trình nông nghiệp và giao thông tỉnh	Đơn vị sự nghiệp
17	Ban Quản lý dự án đầu tư xây dựng tỉnh	Đơn vị sự nghiệp
18	Trung tâm xúc tiến đầu tư, du lịch và thương mại tỉnh	Đơn vị sự nghiệp
19	Quỹ đầu tư phát triển Khánh Hòa	Đơn vị sự nghiệp
20	Trường Đại học Khánh Hòa	Đơn vị sự nghiệp
21	Trường Cao đẳng kỹ thuật công nghệ Nha Trang	Đơn vị sự nghiệp
22	Trường Cao đẳng công nghệ năng lượng Khánh Hòa	Đơn vị sự nghiệp
	Đảng ủy, UBND xã/phường: 07	
1	Phường Bắc Nha Trang	Phường/Xã
2	Phường Tây Nha Trang	Phường/Xã
3	Phường Nam Nha Trang	Phường/Xã
4	UBND phường Nha Trang[6]	Phường/Xã

*** Khu vực II (Đảng ủy, UBND xã/phường): 46**

STT	Tên đơn vị	Ghi chú
1	Phường Bắc Cam Ranh	Phường/Xã
2	Phường Cam Ranh	Phường/Xã
3	Phường Cam Linh	Phường/Xã
4	Phường Ba Ngòi	Phường/Xã
5	Xã Nam Cam Ranh	Phường/Xã
6	Xã Diên Khánh	Phường/Xã

[6] Đảng ủy phường Nha Trang đã thực hiện tại Giai đoạn 01

7	Xã Diên Lạc	Phường/Xã
8	Xã Diên Điền	Phường/Xã
9	Xã Diên Lâm	Phường/Xã
10	Xã Diên Thọ	Phường/Xã
11	Xã Suối Hiệp	Phường/Xã
12	Xã Cam Lâm	Phường/Xã
13	Xã Suối Dầu	Phường/Xã
14	Xã Cam Hiệp	Phường/Xã
15	Xã Cam An	Phường/Xã
16	Xã Bắc Khánh Vĩnh	Phường/Xã
17	Xã Trung Khánh Vĩnh	Phường/Xã
18	Xã Tây Khánh Vĩnh	Phường/Xã
19	Xã Nam Khánh Vĩnh	Phường/Xã
20	Xã Khánh Vĩnh	Phường/Xã
21	Xã Khánh Sơn	Phường/Xã
22	Xã Tây Khánh Sơn	Phường/Xã
23	Xã Đông Khánh Sơn	Phường/Xã

*** Khu vực III (Đảng ủy, UBND xã/phường): 26**

STT	Tên đơn vị	Ghi chú
1	Phường Ninh Hòa	Phường/Xã
2	Phường Đông Ninh Hòa	Phường/Xã
3	Phường Hòa Thắng	Phường/Xã
4	Xã Bắc Ninh Hòa	Phường/Xã
5	Xã Tân Định	Phường/Xã
6	Xã Nam Ninh Hòa	Phường/Xã
7	Xã Tây Ninh Hòa	Phường/Xã
8	Xã Hòa Trí	Phường/Xã
9	Xã Đại Lãnh	Phường/Xã
10	Xã Tu Bông	Phường/Xã
11	Xã Vạn Thắng	Phường/Xã
12	Xã Vạn Ninh	Phường/Xã
13	Xã Vạn Hưng	Phường/Xã

*** Khu vực IV (Đảng ủy, UBND xã/phường): 47**

STT	Tên đơn vị	Ghi chú
1	Phường Phan Rang	Phường/Xã
2	Phường Đông Hải	Phường/Xã
3	Phường Ninh Chử	Phường/Xã
4	Phường Bảo An	Phường/Xã
5	Phường Đô Vinh	Phường/Xã
6	Xã Ninh Phước	Phường/Xã

7	Xã Phước Hữu	Phường/Xã
8	Xã Phước Hậu	Phường/Xã
9	Xã Cà Ná	Phường/Xã
10	Xã Phước Hà	Phường/Xã
11	Xã Phước Dinh	Phường/Xã
12	Xã Ninh Hải	Phường/Xã
13	Xã Xuân Hải	Phường/Xã
14	Xã Vĩnh Hải	Phường/Xã
15	Xã Thuận Bắc	Phường/Xã
16	Xã Công Hải	Phường/Xã
17	Xã Ninh Sơn	Phường/Xã
18	Xã Lâm Sơn	Phường/Xã
19	Xã Anh Dũng	Phường/Xã
20	Xã Mỹ Sơn	Phường/Xã
21	Xã Bác Ái Đông	Phường/Xã
22	Xã Bác Ái	Phường/Xã
23	Xã Bác Ái Tây	Phường/Xã
24	UBND Xã Thuận Nam[7]	Phường/Xã

[7] Đảng ủy xã Thuận Nam đã thực hiện tại Giai đoạn 01