

*

Số: -KH/TBANM

Nghệ An, ngày tháng 6 năm 2026

KẾ HOẠCH

**Kiểm tra, đánh giá công tác bảo đảm an ninh, an toàn
hệ thống thông tin trên địa bàn tỉnh Nghệ An năm 2026**

Thực hiện Kế hoạch số 04-KH/BCĐTW ngày 05/01/2026 của Ban Chỉ đạo Trung ương về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số về bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong hệ thống chính trị và Chương trình hành động số 24-CTr/TU ngày 22/4/2026 của Ban Thường vụ Tỉnh ủy Nghệ An về thực hiện Chỉ thị số 57-CT/TW ngày 31/12/2025 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, Tiểu ban An ninh mạng tỉnh Nghệ An ban hành Kế hoạch kiểm tra, đánh giá công tác bảo đảm an ninh, an toàn đối với hệ thống thông tin trên địa bàn tỉnh Nghệ An năm 2026 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 đối với công tác bảo đảm an toàn thông tin trong các hoạt động ứng dụng công nghệ thông tin. 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.

- Kiểm tra, đánh giá thực trạng công tác bảo đảm an toàn an ninh mạng đối với: 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); 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.

- Kiểm tra, đánh giá an ninh, an toàn đối với các hệ thống thông tin thuộc quản lý của cơ quan Đảng, Nhà nước trên địa bàn tỉnh Nghệ An sau khi thực hiện mô hình chính quyền địa phương 02 cấp, đặc biệt là các hệ thống thông tin cấp độ 3 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

- 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

1.1. Đối tượng kiểm tra

Kiểm tra việc tuân thủ quy định pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ đối với các đơn vị:

- Cấp tỉnh: Sở Xây dựng, sở Y tế, Trường Chính trị tỉnh.

- Cấp phường, xã: Phường Vinh Hưng, Vinh Lộc, Tân Mai, Thái Hòa, xã Quỳnh Văn, Quỳnh Anh, Hùng Châu, Đức Châu, Quỳnh Hợp, Thần Lĩnh, Kim Liên, Vạn An, Đô Lương.

1.2. Đối tượng rà quét, đánh giá an ninh an toàn

- Cấp tỉnh: Rà quét, đánh giá an ninh, an toàn đối với 100% hệ thống thông tin cấp độ 3 do các sở chủ trì được giao chủ trì thuê dịch vụ; hệ thống thông tin của các đơn vị được kiểm tra.

- Cấp phường, xã: Hệ thống thông tin của các đơn vị được kiểm tra.

2. Nội dung kiểm tra, đánh giá

2.1. Đối với đơn vị chủ quản; vận hành hệ thống thông tin

- Kiểm tra, đánh giá việc tuân thủ quy định pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ và triển khai phương án bảo đảm an ninh mạng, an toàn thông tin theo phương án trong Hồ sơ đề xuất cấp độ (nếu có) đối với các hệ thống thông tin thuộc phạm vi quản lý.

- Kiểm tra, đánh giá hệ thống quy chế, quy định; việc bố trí nguồn nhân lực; tổ chức bộ máy chuyên biệt cho công tác đảm bảo an toàn, an ninh mạng.

- Việc lưu trữ nhật ký kết nối, chia sẻ, khai thác thông tin dân cư, khai thác dữ liệu; quản lý tài khoản đăng nhập dùng để khai thác, tra cứu thông tin công dân;

- Đánh giá lại toàn bộ hệ thống kết nối thông qua việc kiểm tra nội dung liên quan đến văn bản quy định, quy chế vận hành, sử dụng hệ thống; sơ đồ thiết kế, thông tin giải pháp bảo mật, cách thức thu thập, lưu trữ, sao lưu nhật ký hoạt động, cấu hình giải pháp bảo mật.

2.2. Đối với hệ thống thông tin

* Kiểm tra, đánh giá việc triển khai, đáp ứng các yêu cầu bảo đảm an toàn hệ thống thông tin theo cấp độ được phê duyệt theo hướng dẫn bảo đảm an ninh, an toàn thông tin và hệ thống thông tin, thiết bị đầu cuối phục vụ triển khai hệ thống dịch vụ công trực tuyến, bao gồm:

- Kiểm tra, đánh giá việc thiết lập cấu hình bảo mật trên thiết bị hệ thống, máy chủ, ứng dụng và cơ sở dữ liệu đáp ứng các yêu cầu an toàn theo phương án được phê duyệt trong Hồ sơ đề xuất cấp độ;

- Kiểm tra, đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống đối với thiết bị hệ thống, máy chủ, ứng dụng

- Kiểm tra, đánh giá an toàn mã nguồn đối với phần mềm nội bộ;

- Kiểm tra, đánh giá an toàn, an ninh đối với thiết bị, phần cứng.

* Tiến hành hướng dẫn, kiểm tra, đánh giá các yêu cầu kỹ thuật theo 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 theo Thông tư số 47/2026/TT-BCA, cụ thể:

- Quản lý nhật ký an ninh mạng:

+ Kiểm tra thời gian lưu trữ nhật ký tối thiểu 12 tháng;

+ Kiểm tra áp dụng công nghệ ghi một lần, đọc nhiều lần hoặc lưu trữ bất biến đối với nhật ký; mã hóa nhật ký ở trạng thái lưu trữ và truyền tải.

+ Kiểm tra việc kết nối, tập trung nhật ký về hệ thống giám sát; đảm bảo đường truyền mã hóa.

- Sao lưu và phục hồi dữ liệu:

+ Kiểm tra việc tuân thủ yêu cầu: 03 bản sao, 02 phương tiện lưu trữ khác nhau, ít nhất 01 bản sao ghi trên vật mạng tin không thể ghi đè, sử dụng kỹ thuật cách ly vật lý.

+ Kiểm tra quản lý vòng đời bản lưu, lưu danh mục toàn bộ bản sao, rà quét mã độc định kỳ 01 lần/06 tháng.

+ Kiểm tra việc xóa, hủy dữ liệu an toàn theo SIST SP 800-88, có sử dụng MFA khi thực hiện xóa bản sao lưu.

2.3. Kiểm tra việc thực hiện Kế hoạch số 33/KH-UBND ngày 16/01/2026 của UBND tỉnh về việc triển khai thi hành Luật Bảo vệ dữ liệu cá nhân

Việc quán triệt, triển khai Kế hoạch số 33/KH-UBND ngày 16/01/2026 của UBND tỉnh Nghệ An về việc triển khai thi hành Luật Bảo vệ dữ liệu cá nhân và các văn bản liên quan. Việc ban hành kế hoạch, văn bản chỉ đạo, phân công trách nhiệm; bố trí đầu mối hoặc bộ phận phụ trách bảo vệ dữ liệu cá nhân. Việc ban hành, rà soát, sửa đổi, bổ sung quy chế, quy trình, quy định nội bộ liên quan đến dữ liệu cá nhân. Việc thực hiện các biện pháp bảo vệ dữ liệu cá nhân trong quản lý, vận hành hệ thống thông tin, cơ sở dữ liệu, ứng dụng, dịch vụ số.

2.4. Kiểm tra việc chấp hành các quy định về an toàn, bảo mật dữ liệu, bảo vệ bí mật nhà nước trên môi trường mạng

- Việc triển khai, phổ biến quán triệt văn bản; việc thực hiện chế độ thông tin, báo cáo liên quan công tác bảo vệ BMNN trên không gian mạng tại cơ quan, đơn vị, địa phương.

- Việc thực hiện các quy định bảo vệ BMNN, gồm: xác định BMNN và độ mật của BMNN; vận chuyển, giao nhận, sao chụp, lưu trữ, bảo quản, cung cấp, tiêu hủy, điều chỉnh độ mật và giải mật tài liệu, vật chứa BMNN trên môi trường mạng.

- Quản lý sử dụng chữ ký số, sản phẩm mật mã, kiểm soát truy cập, lưu trữ an toàn. Quy trình thực hiện gửi, nhận quản lý văn bản mật trong môi trường mạng.

- Việc lưu trữ, soạn thảo tài liệu chứa BMNN trên máy có lịch sử kết nối internet, máy tính và các thiết bị lưu trữ ngoại vi có lưu trữ, soạn thảo, truyền đưa, tài liệu BMNN;

- Công tác kiểm tra, khắc phục, xử lý các vụ việc, xử lý cán bộ vi phạm liên quan đến lộ, mất BMNN tại cơ quan, đơn vị, địa phương (nếu có).

2.5. Kiểm tra, đánh giá an toàn thông tin, an ninh mạng đối với các hệ thống thông tin cấp độ 3

Công an tỉnh hợp đồng với các đơn vị có năng lực, chuyên môn về an toàn thông tin thuê dịch vụ rà quét lỗ hổng bảo mật, kiểm thử đối với các hệ thống thông tin cấp độ 3 trên địa bàn tỉnh, đặc biệt là hệ thống thông tin quan trọng, trọng yếu, làm cơ sở để đánh giá an ninh, an toàn, đề xuất các giải pháp bảo đảm an ninh mạng, kịp thời khắc phục các tồn tại, hạn chế.

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*).

- Trên cơ sở hồ sơ đề xuất cấp độ đối với hệ thống thông tin, tiến hành kiểm tra thực trạng hệ thống thông tin đối chiếu với bản thuyết minh trong hồ sơ đề xuất cấp độ đã được cơ quan có thẩm quyền phê duyệt.

- Đoàn kiểm tra tổ chức kiểm tra thực tế, đánh giá việc tuân thủ quy định pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ và triển khai phương án bảo đảm an ninh mạng, an toàn thông tin theo phương án trong Hồ sơ đề xuất cấp độ đối với các hệ thống thông tin thuộc phạm vi quản lý; việc triển khai, đáp ứng các yêu cầu bảo đảm an toàn hệ thống thông tin theo cấp độ được phê duyệt; việc thực hiện các quy định bảo vệ BMNN tại đơn vị.

- Hợp đồng với đơn vị có năng lực bảo đảm an toàn, an ninh mạng sử dụng chuyên gia, dịch vụ triển khai rà quét, kịp thời phát hiện các lỗ hổng bảo mật, kiến nghị khắc phục và trang bị các giải pháp an toàn đối với hệ thống thông tin, đảm bảo hoạt động ổn định.

- 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.

- 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.

3. Thời gian kiểm tra

- Dự kiến từ Quý III năm 2026; sau khi kết thúc kiểm tra, Đoàn kiểm tra tập hợp báo cáo kết quả về Tiểu ban an ninh mạng tỉnh.
- Giao Văn phòng Tiểu ban An ninh mạng tỉnh thông báo lịch kiểm tra đến các đơn vị, địa phương.

III- THÀNH PHẦN ĐOÀN KIỂM TRA

1. Đồng chí 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 cán bộ.
- Giao Văn phòng Tiểu ban An ninh mạng tỉnh tham mưu Quyết định thành lập Đoàn kiểm tra theo quy định.

IV- KINH PHÍ

Giao Sở Tài chính tham mưu UBND tỉnh bố trí nguồn kinh phí phục vụ công tác kiểm tra theo đúng quy định của pháp luật.

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; tham mưu Quyết định 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.
- Tham mưu thuê dịch vụ công nghệ thông tin tổ chức kiểm tra, đánh giá an ninh, an toàn đối với các hệ thống thông tin thuộc quản lý của cơ quan Đảng, Nhà nước trên địa bàn tỉnh, đặc biệt là các hệ thống thông tin cấp độ 3.
- 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 Tài chính: Phối hợp Công an tỉnh lập dự toán, tham mưu UBND tỉnh bố trí nguồn kinh phí phục vụ công tác kiểm tra, đánh giá an ninh, an toàn đối với hệ thống thông tin theo quy định.

3. Các cơ quan, đơn vị, địa phương

- Các Sở, ngành, cơ quan, đơn vị địa phương chủ động xây dựng báo cáo tự kiểm tra việc tuân thủ quy định pháp luật về bảo đảm an toàn hệ thống

thông tin theo cấp độ và bảo vệ bí mật nhà nước trên không gian mạng (*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 **trước ngày 25/6/2026** để tổng hợp.

- 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 gửi kèm báo cáo tự kiểm tra về Công an tỉnh phục vụ Đoàn kiểm tra.

- Các đơn vị chủ quản, đơn vị được giao chủ trì thuê dịch vụ của các hệ thống thông tin cấp độ 3 có trách nhiệm thông báo cho đơn vị vận hành hệ thống thông tin chủ động phối hợp với Đoàn kiểm tra tiến hành rà quét, đánh giá an ninh, an toàn đối với hệ thống thông tin khi có yêu cầu.

Căn cứ Kế hoạch này, đề nghị Thủ trưởng các sở, ban, ngành, đơn vị, địa phương có liên quan triển khai thực hiện nghiêm túc; quá trình thực hiện có khó khăn, vướng mắc các đơn vị, địa phương kịp thời trao đổi về Cơ quan Thường trực Tiểu ban An ninh mạng tỉnh (*qua đồng chí Đại úy Lê Tiến Nhật - Cán bộ Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh, số điện thoại: 0916.852.588*) để được hướng dẫn; trường hợp vượt quá thẩm quyền, Cơ quan Thường trực Tiểu ban báo cáo Trưởng Tiểu ban An ninh mạng tỉnh xem xét, quyết định./.

Nơi nhận:

- Đ/c Trưởng Tiểu ban,
- P. Trưởng TB Thường trực; } (để báo cáo)
- CA tỉnh, Sở Tài chính;
- Các đơn vị, địa phương;
- Lưu: VT, CAT (PA05).

**KT. TRƯỞNG TIỂU BAN
PHÓ TRƯỞNG TIỂU BAN**

**Thiếu tướng Đinh Việt Dũng
GIÁM ĐỐC CÔNG AN TỈNH**

PHỤ LỤC
ĐỀ CƯƠNG BÁO CÁO TỰ KIỂM TRA, ĐÁNH GIÁ CÔNG TÁC
BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN THEO CẤP ĐỘ
(Kèm theo Kế hoạch số -KH/TBANM ngày /6/2026 của
Tiểu ban An ninh mạng tỉnh Nghệ An)

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- BT TTTT 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. Việc quán triệt, triển khai Kế hoạch số 33/KH-UBND ngày 16/01/2026 của UBND tỉnh Nghệ An về việc triển khai thi hành Luật Bảo vệ dữ liệu cá nhân và các văn bản liên quan.

10. 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;

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

12. 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.

- 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