ỦY BAN NHÂN DÂN **TỈNH QUẢNG TRỊ**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 2971/KH-UBND	*Quảng Trị, ngày 02 tháng 12 năm 2025*

KẾ HOẠCH
Bảo đảm an toàn, an ninh mạng giai đoạn 2025 - 2027, tầm nhìn 2030 trên địa bàn tỉnh Quảng Trị

Thực hiện Chiến lược An toàn, an ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030 và Kế hoạch hành động số 09-KH/TU ngày 31/7/2025 của Ban Thường vụ Tỉnh ủy Quảng Trị thực hiện Nghị quyết số 57-NQ/TW ngày 22/12/2024 của Bộ Chính trị về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia trên địa bàn tỉnh Quảng Trị; Ủy ban nhân dân (UBND) tỉnh ban hành kế hoạch bảo đảm an toàn, an ninh mạng trên địa bàn tỉnh Quảng Trị giai đoạn 2025 - 2027, tầm nhìn 2030 như sau:

I. CĂN CỨ PHÁP LÝ

Quyết định số 749/QĐ-TTg ngày 03/6/2020 của Thủ tướng Chính phủ về việc phê duyệt Chương trình chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030;

Quyết định số 942/QĐ-TTg ngày 15/6/2021 của Thủ tướng Chính phủ phê duyệt Chiến lược phát triển Chính phủ điện tử hướng tới Chính phủ số giai đoạn 2021-2025, tầm nhìn đến năm 2030;

Quyết định số 411/QĐ-TTg ngày 31/3/2022 của Thủ tướng Chính phủ phê duyệt Chiến lược quốc gia phát triển kinh tế số và xã hội số đến năm 2025, định hướng đến năm 2030;

Quyết định số 964/QĐ-TTg ngày 10/8/2022 của Thủ tướng Chính phủ phê duyệt Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030;

Quyết định số 1562/QĐ-TTg ngày 18/7/2025 của Thủ tướng Chính phủ về bảo đảm liên thông, đồng bộ, bí mật nhà nước trong chuyển đổi số của hệ thống chính trị;

Công văn số 1406/TTg-KSTT ngày 30/10/2025 của Thủ tướng Chính phủ về việc triển khai công tác bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu;

Kế hoạch hành động số 09-KH/TU ngày 31/7/2025 của Ban Thường vụ Tỉnh ủy Quảng Trị thực hiện Nghị quyết số 57-NQ/TW ngày 22/12/2024 của Bộ Chính trị về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia trên địa bàn tỉnh Quảng Trị;

Kế hoạch số 635/KH-UBND ngày 22/8/2025 của UBND tỉnh Quảng Trị về thực hiện Nghị quyết số 57-NQ/TW ngày 22/12/2024 của Bộ Chính trị, Nghị quyết số 71/NQ-CP ngày 01/4/2025 của Chính phủ và Kế hoạch hành động số 09-KH/TU ngày 31/7/2025 của Ban Thường vụ Tỉnh ủy về thực hiện Nghị quyết số 57-NQ/TW của Bộ Chính trị trên địa bàn Quảng Trị.

II. QUAN ĐIỂM VÀ MỤC TIÊU, YÊU CẦU

1. Quan điểm

- An toàn, an ninh mạng là trọng tâm của quá trình chuyển đổi số, là trụ cột quan trọng tạo lập niềm tin số và sự phát triển thịnh vượng trong kỷ nguyên số. An toàn, an ninh mạng là nhiệm vụ trọng yếu, thường xuyên, lâu dài nhằm khởi tạo và duy trì môi trường mạng an toàn, lành mạnh, tin cậy cho các cơ quan, tổ chức, doanh nghiệp và mỗi người dân. Đầu tư cho an toàn, an ninh mạng là đầu tư cho phát triển bền vững và tạo ra giá trị.

- Bảo đảm an toàn, an ninh mạng là then chốt để chuyển đổi số thành công và bền vững, đồng thời là phần xuyên suốt, không thể tách rời của chuyển đổi số. Mọi thiết bị, sản phẩm, phần mềm, hệ thống thông tin, dự án đầu tư về công nghệ thông tin đều có cấu phần bắt buộc về an toàn, an ninh mạng ngay từ khi thiết kế.

2. Mục tiêu tổng quát

- Bảo đảm an toàn các hệ thống thông tin trên địa bàn tỉnh trước các nguy cơ tấn công mạng, phá hoại hệ thống thông tin; chủ động, sẵn sàng ứng phó với các nguy cơ, thách thức từ không gian mạng nhằm bảo vệ vững chắc chủ quyền, lợi ích, quốc phòng, an ninh quốc gia, trật tự an toàn xã hội; bảo vệ chủ quyền quốc gia trên không gian mạng và công cuộc chuyển đổi số, quyền và lợi ích hợp pháp của tổ chức, cá nhân trên không gian mạng.

- Duy trì, nâng cao năng lực, thứ hạng về an toàn, an ninh mạng của tỉnh.

3. Mục tiêu đến năm 2030

- Phát triển, kiện toàn, nâng cao năng lực lực lượng bảo đảm an toàn, an ninh mạng của tỉnh.

- Thực hiện bảo đảm an toàn, an ninh mạng theo quy định của pháp luật về an toàn, an ninh mạng, cụ thể:

+ 100% hệ thống thông tin trên địa bàn tỉnh được xác định và đảm bảo an toàn thông tin theo cấp độ.

+ 100% các đơn vị trong tỉnh triển khai đảm bảo an toàn thông tin theo mô hình 4 lớp[1]. Đối với các hệ thống thông tin cấp độ 3 trở lên, tổ chức giám sát, bảo vệ đầy đủ các lớp: lớp mạng, lớp ứng dụng, lớp cơ sở dữ liệu và lớp thiết bị đầu cuối.

+ 100% hệ thống thông tin được triển khai giám sát an toàn, an ninh mạng.

+ 100% hệ thống thông tin được triển khai phòng chống mã độc.

+ 100% hệ thống thông tin được kiểm tra, đánh giá an toàn thông tin mạng.

+ 100% cán bộ làm công tác an toàn thông tin được đào tạo, tập huấn, diễn tập ứng cứu khắc phục sự cố.

+ 100% các hệ thống thông tin hoạt động trên mạng Internet có chức năng đăng nhập áp dụng phương thức xác thực đa yếu tố.

---

[1] Gồm: Lực lượng tại chỗ (Lớp 1); Tổ chức hoặc thuê doanh nghiệp giám sát, bảo vệ chuyên nghiệp (Lớp 2); Tổ chức hoặc thuê doanh nghiệp độc lập kiểm tra, đánh giá định kỳ (Lớp 3); Kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia (Lớp 4).

+ 100% cán bộ, công chức, viên chức, người lao động được tham gia các hoạt động nâng cao nhận thức, kỹ năng và công cụ bảo đảm an toàn, an ninh mạng.

+ 100% đơn vị xử lý dữ liệu cá nhân xây dựng quy định về bảo vệ dữ liệu cá nhân.

+ Nghiên cứu, đề xuất các dự án để triển khai tổng thể, đồng bộ các phương án bảo đảm an toàn, an ninh mạng đã được phê duyệt.

Công tác bảo đảm an toàn, an ninh mạng của tỉnh đáp ứng đầy đủ quy định của pháp luật về an toàn, an ninh mạng; hỗ trợ và góp phần triển khai thành công quá trình chuyển đổi số trên địa bàn tỉnh.

4. Yêu cầu

- Phát huy sức mạnh của cả hệ thống chính trị và toàn xã hội, nhất là mối quan hệ giữa Nhà nước, doanh nghiệp và người dân trong bảo đảm an toàn, an ninh mạng. Chuyển đổi căn bản về nhận thức và cách làm, xây dựng và phát triển lực lượng bảo đảm an toàn, an ninh mạng hiện đại, chuyên nghiệp, đáp ứng yêu cầu thực tiễn.

- Các nhiệm vụ được xác định có trọng tâm, lộ trình thực hiện đảm bảo tính khả thi gắn với phân công trách nhiệm cụ thể, phù hợp với chức năng, nhiệm vụ các đơn vị; đồng thời bảo đảm sự phối hợp chặt chẽ, hiệu quả, kịp thời giữa các đơn vị trong triển khai thực hiện nhiệm vụ; chủ động giải quyết kịp thời những khó khăn, vướng mắc trong quá trình triển khai bảo đảm hoàn thành các nhiệm vụ đề ra.

- Thống nhất với các mục tiêu, nhiệm vụ bảo đảm an toàn, an ninh mạng đến năm 2030 mà UBND tỉnh đã ban hành tại Kế hoạch số 635/KH-UBND ngày 22/8/2025.

III. NHIỆM VỤ, GIẢI PHÁP

1. Nhiệm vụ thường xuyên

1.1. Tăng cường vai trò lãnh đạo của Đảng, quản lý của Nhà nước

- Thống nhất nhận thức trong toàn thể cán bộ, công chức, viên chức và người lao động về bảo đảm an toàn, an ninh mạng là trách nhiệm của toàn bộ các đơn vị, là trách nhiệm của mỗi cán bộ, công chức, viên chức, người lao động.

- Thường xuyên phổ biến, quán triệt chủ trương của Đảng, chính sách, pháp luật của Nhà nước về an toàn, an ninh mạng, coi đây là nhiệm vụ chính trị quan trọng.

- Nâng cao nhận thức, trách nhiệm của các tổ chức, cá nhân trong công tác bảo đảm an toàn, an ninh mạng. Người đứng đầu cấp ủy trực tiếp lãnh đạo, chỉ đạo và chịu trách nhiệm về công tác an toàn, an ninh mạng, chủ động rà soát, xác định rõ những vấn đề trọng tâm, trọng điểm để chỉ đạo thực hiện hiệu quả.

- Phát huy sự tham gia có hiệu quả của các tổ chức, cá nhân sử dụng hệ thống công nghệ thông tin của tỉnh trong công tác bảo đảm an toàn, an ninh mạng và chủ động ứng phó với các nguy cơ, thách thức từ không gian mạng.

1.2. Hoàn thiện văn bản về an toàn, an ninh mạng

Căn cứ vào tình hình triển khai thực tế tại địa phương để rà soát, đề xuất xây dựng, sửa đổi, bổ sung văn bản về bảo đảm an toàn, an ninh mạng cho giao dịch điện tử, chuyển đổi số, hạ tầng số, nền tảng số, bảo vệ thông tin cá nhân trên mạng bảo đảm phù hợp với các văn bản quy phạm pháp luật hiện hành về an toàn, an ninh mạng.

1.3. Bảo vệ chủ quyền quốc gia trên không gian mạng

Phối hợp chặt chẽ giữa các lực lượng Quân sự, Công an, Khoa học và Công nghệ, các cơ quan liên quan chủ động bảo vệ độc lập, chủ quyền quốc gia trên không gian mạng theo chức năng, nhiệm vụ được giao.

1.4. Bảo vệ hạ tầng số, nền tảng số, dữ liệu số, cơ sở hạ tầng không gian mạng

- Đẩy mạnh hoạt động bảo đảm an toàn, an ninh mạng trong quá trình thiết kế, xây dựng, vận hành, khai thác cơ sở hạ tầng số; tuân thủ tiêu chuẩn, quy chuẩn kỹ thuật, hướng dẫn nghiệp vụ của Bộ Công an, Bộ Khoa học và Công nghệ và quy định của pháp luật về an toàn, an ninh mạng; gắn kết công tác bảo đảm an toàn, an ninh mạng với công tác triển khai chuyển đổi số, ứng dụng công nghệ thông tin, phát triển chính quyền điện tử hướng tới chính quyền số, phát triển đô thị thông minh, kinh tế số và xã hội số.

- Chủ động giám sát, phát hiện và công bố hành vi vi phạm quy định pháp luật của Việt Nam thuộc phạm vi quản lý trên các nền tảng số. Xử lý theo thẩm quyền hoặc phối hợp với đơn vị chức năng của Bộ Công an, Bộ Khoa học và Công nghệ xử lý tổ chức, cá nhân vi phạm, gỡ bỏ thông tin vi phạm trên các nền tảng số.

- Rà soát, nâng cấp Trung tâm dữ liệu điện tử và Kho dữ liệu dùng chung của tỉnh bảo đảm đạt tiêu chuẩn quy định. Triển khai các biện pháp bảo đảm an toàn hệ thống thông tin theo cấp độ đối với Trung tâm dữ liệu điện tử và Kho dữ liệu dùng chung của tỉnh.

- Tăng cường công tác chỉ đạo, kiểm tra, đánh giá các doanh nghiệp cung cấp dịch vụ nền tảng số trên địa bàn trong thực thi trách nhiệm bảo đảm an toàn thông tin mạng, an ninh mạng theo chức năng, nhiệm vụ được giao.

- Cung cấp các dịch vụ viễn thông, Internet an toàn. Bảo đảm an toàn thông tin mạng trong toàn bộ quá trình thiết kế, xây dựng, khai thác, vận hành các loại hình dịch vụ. Ưu tiên sử dụng sản phẩm an toàn, an ninh mạng của Việt Nam ("Make in Viet Nam")

1.5. Bảo vệ hệ thống thông tin của các cơ quan Đảng, Nhà nước

- Nâng cao trách nhiệm tự bảo vệ hệ thống thông tin thuộc phạm vi quản lý. Gắn trách nhiệm của người đứng đầu cơ quan, đơn vị chủ quản hệ thống thông tin với trách nhiệm bảo đảm an toàn, an ninh mạng.

- Xây dựng, cập nhật, vận hành hệ thống thông tin theo tiêu chuẩn, quy chuẩn kỹ thuật về an toàn, an ninh mạng.

- Rà soát, lập hồ sơ đề nghị đưa các hệ thống thông tin trọng yếu, phù hợp với quy định của pháp luật vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

- Thực hiện nghiêm túc các quy định pháp luật về bảo vệ an ninh mạng. Chủ động xây dựng kế hoạch, tổ chức kiểm tra ninh mạng đối với hệ thống thông tin quan trọng của các cơ quan Đảng, Nhà nước trên địa bàn tỉnh. Phối hợp với chủ quản hệ thống thông tin khắc phục, xử lý nguy cơ đe dọa an ninh mạng, sự cố an ninh mạng, điểm yếu, lỗ hổng bảo mật, phần cứng độc hại.

- Xác định cấp độ, trách nhiệm bảo đảm an toàn hệ thống thông tin theo từng cấp độ và triển khai mô hình "4 lớp" trước khi đưa vào sử dụng; nhất là hệ thống thông tin của các lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin.

- Chủ động giám sát, kịp thời phát hiện nguy cơ mất an toàn, an ninh mạng trong quá trình thi công, lắp đặt thiết bị trong các hệ thống thông tin. Ưu tiên sử dụng sản phẩm, giải pháp an toàn, an ninh mạng "Make in Viet Nam".

- Đầu tư nguồn lực, thường xuyên nâng cấp hệ thống, cập nhật bản quyền, nâng cao nhận thức và kỹ năng an toàn, an ninh mạng cho cán bộ, công chức, viên chức và người lao động.

- Tối thiểu mỗi năm tổ chức 01 lần diễn tập, hướng dẫn, kiểm tra, ứng phó và ứng cứu sự cố an toàn, an ninh mạng; nhất là ứng phó và ứng cứu sự cố an toàn thông tin cho các lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin.

- Phối hợp với cơ quan chuyên trách về an ninh mạng của Bộ Công an kết nối với Trung tâm An ninh mạng quốc gia để giám sát an ninh mạng.

1.6. Tạo lập niềm tin số, xây dựng môi trường mạng trung thực, văn minh, lành mạnh và phòng chống vi phạm pháp luật trên không gian mạng

- Thiết lập, cập nhật thông tin đường dây nóng, hệ thống tiếp nhận, xử lý thông tin về tội phạm mạng từ không gian mạng để quần chúng Nhân dân phản ánh kịp thời, trực tiếp thông tin hành vi vi phạm pháp luật trên không gian mạng.

- Đổi mới nội dung, hình thức, biện pháp xây dựng phong trào toàn dân bảo vệ an ninh Tổ quốc phù hợp với thực tiễn chuyển đổi số. Phát huy vai trò của Thế trận An ninh nhân dân, Thế trận Quốc phòng toàn dân trên không gian mạng. Giám sát, phát hiện xử lý tin giả, thông tin vi phạm pháp luật trong phạm vi quản lý.

- Phát triển các website, trang mạng xã hội, ứng dụng trên môi trường mạng uy tín, nhiều tương tác để tuyên truyền, định hướng thông tin, dư luận và phản bác hiệu quả các thông tin tiêu cực về đất nước, con người Việt Nam.

1.7. Đào tạo và phát triển nguồn nhân lực

- Xây dựng kế hoạch phát triển, nâng cao chất lượng nguồn nhân lực bảo đảm an toàn, an ninh mạng của tỉnh.

- Tham gia các chương trình đào tạo về an toàn, an ninh mạng do các cơ quan chức năng tổ chức.

- Ưu tiên bố trí nguồn lực (nhân lực, kinh phí) và điều kiện để triển khai hoạt động bảo đảm an toàn, an ninh mạng trong hoạt động nội bộ của cơ quan, tổ chức

và lĩnh vực quản lý. Có hình thức khen thưởng kịp thời, phù hợp đối với tổ chức, cá nhân có cống hiến về bảo đảm an toàn, an ninh mạng.

1.8. Tuyên truyền, phổ biến, nâng cao nhận thức và kỹ năng an toàn, an ninh mạng

- Cung cấp kịp thời các thông tin chính thống để cán bộ, công chức, viên chức, người lao động, người dân, doanh nghiệp nắm bắt, cùng phản biện tin giả, thông tin vi phạm pháp luật trên môi trường mạng.

- Tổ chức triển khai các kế hoạch tuyên truyền, phổ biến thói quen, trách nhiệm, kỹ năng an toàn, an ninh mạng cho cán bộ, công chức, viên chức, người lao động khi tham gia hoạt động trên không gian mạng.

- Các cơ sở giáo dục, đào tạo xây dựng chương trình, kế hoạch học tập, rèn luyện kỹ năng tư duy phản biện cho sinh viên về an toàn, an ninh mạng đối với các thông tin sai lệch trên không gian mạng.

- Các tổ chức truyền thông, báo chí thường xuyên tuyên truyền, phổ biến chủ trương của Đảng, chính sách, pháp luật của Nhà nước về an toàn, an ninh mạng, coi đây là nhiệm vụ chính trị quan trọng; tăng cường thông tin về xu hướng, kiến thức, tình hình, nguy cơ, hậu quả an toàn, an ninh mạng thế giới và Việt Nam.

1.9. Hợp tác quốc tế

Phối hợp với đơn vị chức năng của Bộ Quốc phòng, Bộ Công an, Bộ Khoa học và Công nghệ, Bộ Ngoại giao trong việc tham gia hợp tác với các tổ chức quốc tế, các quốc gia về an toàn, an ninh mạng phù hợp với quy định của pháp luật và đặc thù của địa phương.

1.10. Đầu tư nguồn lực và bảo đảm kinh phí thực hiện

- Bố trí đủ nhân lực chuyên trách, chịu trách nhiệm về an toàn, an ninh mạng trong các cơ quan, tổ chức.

- Đầu tư nguồn lực để xây dựng hệ thống kỹ thuật, công cụ và triển khai các hoạt động bảo đảm an toàn, an ninh mạng và trong hoạt động của cơ quan, tổ chức.

- Ưu tiên bố trí kinh phí từ ngân sách nhà nước để triển khai các nhiệm vụ và xây dựng các hệ thống kỹ thuật hiện đại bảo đảm an toàn, an ninh mạng theo quy định của pháp luật về đầu tư công, pháp luật về ngân sách nhà nước. Bố trí kinh phí chi cho các sản phẩm, dịch vụ an ninh mạng, bảo mật thông tin, dữ liệu đạt tối thiểu 15% tổng kinh phí triển khai đề án, dự án công nghệ thông tin.

2. Nhiệm vụ giai đoạn 2025 - 2027

2.1. Tuyên truyền, phổ biến, nâng cao nhận thức, kỹ năng của cán bộ, công chức, viên chức và người lao động về an toàn, an ninh mạng, bảo vệ dữ liệu cá nhân

Xây dựng chương trình, kế hoạch phát động phong trào học tập trên các nền tảng số; thường xuyên, liên tục phổ cập, nâng cao kiến thức về an toàn thông tin, an ninh mạng, bảo vệ dữ liệu cá nhân.

2.2. Đào tạo, bồi dưỡng kiến thức về an toàn, an ninh mạng

- Triển khai các hoạt động đào tạo, bồi dưỡng, tập huấn chuyên sâu về kiến trúc, hạ tầng, dữ liệu, phân tích dữ liệu, sử dụng dữ liệu hỗ trợ ra quyết định và chỉ đạo điều hành của lãnh đạo các cấp; đào tạo nâng cao trình độ chuyên môn cho đội ngũ chuyên trách chuyển đổi số và an toàn, an ninh mạng.

- Tăng cường trao đổi, làm việc khảo sát và học tập kinh nghiệm trong nước và quốc tế về chuyển đổi số.

- Đảm bảo 100% cán bộ chuyên trách/kiêm nhiệm về an toàn thông tin được định kỳ tham gia các khóa đào tạo, bồi dưỡng kỹ thuật về an toàn, an ninh mạng.

2.3. Xây dựng, rà soát, sửa đổi quy định nội bộ về bảo đảm an toàn, an ninh mạng phù hợp với các quy định về an toàn, an ninh mạng

- Xây dựng Quy chế Quản lý, sử dụng chữ ký số chuyên dùng công vụ, chứng thư chữ ký số chuyên dùng công vụ, thiết bị lưu khóa bí mật và dịch vụ chứng thực chữ ký số chuyên dùng công vụ (cập nhật quy chế nếu có).

- Xây dựng Quy chế Bảo đảm an ninh mạng, an toàn thông tin tỉnh.

- Xây dựng, sửa đổi các quy định, quy trình quản lý vận hành phù hợp với Quy chế Bảo đảm an ninh mạng, an toàn thông tin.

2.4. Chỉ định, kiện toàn bộ phận/lực lượng thực hiện nhiệm vụ về an toàn, an ninh mạng

Xây dựng, trình cấp có thẩm quyền ban hành quyết định, quy định chức năng, nhiệm vụ của đơn vị, bộ phận thực hiện công tác bảo đảm an toàn thông tin và an ninh mạng (cập nhật quy định nếu có).

2.5. Xác định cấp độ an toàn hệ thống thông tin và triển khai phương án bảo đảm an toàn hệ thống thông tin theo cấp độ được phê duyệt

- Hoàn thành phân loại, xác định, phê duyệt đề xuất cấp độ an toàn hệ thống thông tin và phương án bảo đảm an toàn hệ thống thông tin theo cấp độ phù hợp với quy định của pháp luật, tiêu chuẩn quốc gia về an toàn hệ thống thông tin theo cấp độ và hướng dẫn của cơ quan chức năng; triển khai đầy đủ phương án bảo đảm an toàn hệ thống thông tin theo cấp độ các hệ thống thông tin.

- Tiếp tục triển khai phương án bảo đảm an toàn thông tin theo cấp độ và mô hình bảo vệ "4 lớp".

2.6. Điều phối, diễn tập ứng cứu sự cố an toàn, an ninh mạng

- Thành lập Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Quảng Trị.

- Tổ chức huấn luyện, diễn tập thực chiến đảm bảo an toàn các hệ thống thông tin.

- Tổ chức tham gia diễn tập ứng cứu sự cố hệ thống thông tin do cơ quan chức năng tổ chức.

2.7. Phòng chống mã độc tập trung và chia sẻ thông tin mã độc

- Rà soát, thống kê tình hình sử dụng phần mềm bản quyền được cài đặt trên máy tính.

- Tiếp tục tổ chức triển khai hệ thống phòng chống mã độc cho các hệ thống thông tin.

- Tổ chức tổng hợp, chia sẻ thông tin mã độc với hệ thống giám sát an ninh mạng quốc gia.

2.8. Giám sát và chia sẻ thông tin giám sát an toàn, an ninh mạng

- Xây dựng Trung tâm An ninh mạng tỉnh Quảng Trị để giám sát, tổng hợp tình hình an toàn, an ninh mạng của toàn bộ các hệ thống thông tin của tỉnh.

- Tổ chức triển khai giám sát an toàn, an ninh mạng hệ thống thông tin.

- Tổ chức tổng hợp, chia sẻ thông tin giám sát theo hướng dẫn của cơ quan chức năng.

2.9. Kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin

Định kỳ, đột xuất thực hiện kiểm tra, đánh giá an toàn, an ninh mạng và rà soát, thực hiện săn lùng mối nguy hại, khắc phục các điểm yếu, lỗ hổng bảo mật theo quy định của pháp luật, các bộ, ngành liên quan và của tỉnh.

Nội dung kiểm tra, đánh giá:

- Kiểm tra, đánh giá việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ.

- 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.

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

2.10. Bảo vệ dữ liệu

- Triển khai Luật Bảo vệ dữ liệu cá nhân: xây dựng Quy chế Bảo vệ dữ liệu cá nhân.

- Tham gia tập huấn chuyên sâu, bồi dưỡng kiến thức pháp luật, nghiệp vụ xây dựng, phát triển, bảo vệ, quản trị, xử lý, sử dụng dữ liệu.

- Dữ liệu bí mật nhà nước khi liên thông, đồng bộ được phân loại, mã hóa bằng giải pháp bảo mật cơ yếu theo đúng cấp độ bí mật và được xử lý trên các hệ thống đáp ứng yêu cầu bảo mật tương ứng, do cơ quan có thẩm quyền phê duyệt.

- Cơ quan chủ quản dữ liệu, nền tảng, hệ thống thông tin chủ trì xây dựng phương án và tổ chức thực hiện liên thông thuộc phạm vi quản lý bảo đảm các biện pháp bảo vệ dữ liệu cá nhân, bảo vệ bí mật nhà nước theo quy định của pháp luật.

2.11. Các nội dung khác

- Rà soát hiện trạng, tăng cường đầu tư nâng cấp hạ tầng công nghệ thông tin và các giải pháp an toàn thông tin với công nghệ tiên tiến, hiện đại nhằm đảm bảo các hệ thống vận hành ổn định, thông suốt và an ninh an toàn, đáp ứng yêu cầu về bảo đảm an toàn, an ninh mạng phục vụ triển khai Đề án 06.

- Chỉ đạo các công ty, doanh nghiệp thuộc phạm vi quản lý rà soát, đánh giá, có biện pháp tăng cường bảo đảm an toàn, an ninh mạng đối với các hệ thống hạ

tầng thông tin, hệ thống điều khiển công nghiệp và các hệ thống thông tin quan trọng khác do doanh nghiệp quản lý, vận hành, khai thác.

3. Nhiệm vụ trọng tâm giai đoạn 2028 - 2030

- Xây dựng, phát triển lực lượng nòng cốt bảo đảm an toàn, an ninh mạng, bảo vệ dữ liệu cá nhân của tỉnh.

- Xây dựng các chính sách, quy định bảo đảm triển khai công tác an toàn, an ninh mạng đồng bộ, thống nhất trong tỉnh.

- Triển khai phương án bảo đảm an toàn, an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý, bảo đảm đồng bộ, thống nhất, tập trung, có sự chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư trùng lặp.

- Ứng dụng trí tuệ nhân tạo dựa trên dữ liệu lớn trong bảo đảm an toàn thông tin mạng, an ninh mạng, đặc biệt trong việc giám sát hệ thống, phát hiện, phòng chống xâm nhập mạng.

- Tiếp tục thực hiện các nhiệm vụ giai đoạn 2025-2027.

(Chi tiết các nhiệm vụ cụ thể tại Phụ lục kèm theo).

IV. TỔ CHỨC THỰC HIỆN

1. Tiểu ban An toàn, an ninh mạng tỉnh điều phối chung sự phối hợp giữa 04 lực lượng gồm Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh, Sở Khoa học và Công nghệ và Ban Tuyên giáo và Dân vận Tỉnh ủy. Các lực lượng chủ động, phối hợp thực hiện các nội dung trong Kế hoạch theo chức năng, nhiệm vụ được giao.

2. Công an tỉnh - Cơ quan thường trực Tiểu ban An toàn, an ninh mạng tỉnh chủ trì theo dõi, đánh giá, đôn đốc các cơ quan, đơn vị, địa phương triển khai thực hiện có hiệu quả công tác bảo đảm an toàn, an ninh mạng và các nhiệm vụ được giao tại Kế hoạch này. Định kỳ, đột xuất tổng hợp tình hình, kết quả triển khai thực hiện của các sở, ban, ngành, UBND xã, phường, đặc khu và tham mưu báo cáo Chính phủ theo quy định; tham mưu Chủ tịch UBND tỉnh điều chỉnh Kế hoạch đảm bảo phù hợp với Quy chế Bảo đảm an ninh mạng, an toàn thông tin tỉnh và tình hình thực tiễn khi xét thấy cần thiết.

3. Đề nghị Văn phòng Tỉnh ủy chủ trì, phối hợp Công an tỉnh tham mưu triển khai biện pháp bảo đảm an toàn, an ninh mạng các hệ thống thông tin (trừ các hệ thống được bảo vệ theo chức năng, nhiệm vụ của Ban Cơ yếu Chính phủ và Bộ Quốc phòng) thuộc Tỉnh ủy, Đảng ủy các xã, phường, đặc khu theo quan điểm chỉ đạo tại Kế hoạch số 02-KH/BCĐTW ngày 19/6/2025 của Ban Chỉ đạo Trung ương về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số; Thông báo kết luận số 44-TB/TGV ngày 12/9/2025 của Tổ giúp việc Ban Chỉ đạo Trung ương về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số.

4. Sở Tài chính chủ trì tham mưu, hướng dẫn cơ chế, chính sách về tài chính, ngân sách, kế hoạch, đầu tư, cân đối, bố trí nguồn lực tài chính từ ngân sách nhà nước và huy động các nguồn lực khác bảo đảm cho việc triển khai, thực hiện Kế hoạch này.

5. Các sở, ban, ngành, UBND các xã, phường, đặc khu căn cứ chức năng, nhiệm vụ được giao xây dựng kế hoạch triển khai thực hiện nghiêm túc, hiệu quả. Định kỳ hàng năm *(trước ngày 15/11)*, báo cáo Chủ tịch UBND tỉnh *(qua Công an tỉnh)* về tình hình, kết quả triển khai thực hiện và khó khăn, vướng mắc, kiến nghị, đề xuất.

Trên đây là Kế hoạch bảo đảm an toàn, an ninh mạng trên địa bàn tỉnh Quảng Trị giai đoạn 2025 - 2027, tầm nhìn 2030. Trong quá trình triển khai thực hiện, nếu có khó khăn, vướng mắc, các cơ quan, đơn vị, địa phương phản ánh về UBND tỉnh (qua Công an tỉnh) để xem xét, chỉ đạo./.

Nơi nhận:
- Văn phòng Chính phủ;
- Thường trực Tỉnh ủy;
- Thường trực HĐND tỉnh;
- Chủ tịch, các PCT UBND tỉnh;
- Ban Tuyên giáo và Dân vận Tỉnh ủy;
- Các Văn phòng: Tỉnh ủy, Đoàn ĐBQH và HĐND tỉnh, UBND tỉnh;
- Các sở, ban, ngành, đoàn thể cấp tỉnh;
- UBND các xã, phường, đặc khu;
- Công an tỉnh;
- Lưu: VT, NC.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Lê Hồng Vinh

Phụ lục

NHIỆM VỤ TRIỂN KHAI KẾ HOẠCH BẢO ĐẢM AN TOÀN, AN NINH MẠNG GIAI ĐOẠN 2025 - 2027, TẦM NHÌN 2030 TRÊN ĐỊA BÀN TỈNH QUẢNG TRỊ

(Kèm theo Kế hoạch số 2197../KH-UBND ngày 02/12/2025 của UBND tỉnh Quảng Trị)

STT	Nội dung thực hiện	Đơn vị chủ trì	Đơn vị phối hợp	Thời gian hoàn thành
1	**Tuyên truyền, phổ biến, nâng cao nhận thức, kỹ năng của cán bộ, công chức, viên chức và người lao động về an toàn, an ninh mạng, bảo vệ dữ liệu cá nhân**			
1.1	Tổ chức các hoạt động tuyên truyền, phổ biến nâng cao nhận thức của cán bộ, công chức, viên chức và người lao động tại đơn vị, như: hội nghị, sinh hoạt chuyên đề	Các đơn vị trên địa bàn tỉnh	Công an tỉnh	Quý IV năm 2025; Thường xuyên
2	**Đào tạo, bồi dưỡng kiến thức về an toàn, an ninh mạng**			
2.1	Tổ chức đào tạo, bồi dưỡng kiến thức, kỹ năng an toàn, an ninh mạng cho cán bộ, công chức, viên chức và người lao động của cơ quan, đơn vị trong tỉnh	Công an tỉnh	Các đơn vị liên quan	Năm 2026; Thường xuyên
2.2	Đào tạo, hướng dẫn sử dụng các nền tảng quản lý bảo đảm an toàn hệ thống thông tin: nền tảng Hỗ trợ quản lý bảo đảm an toàn hệ thống thông tin theo cấp độ; nền tảng Hỗ trợ điều phối, ứng cứu sự cố; nền tảng Hỗ trợ điều tra số	Công an tỉnh; Đội ứng cứu sự số an toàn thông tin mạng	Các đơn vị liên quan	Năm 2026; Thường xuyên
2.3	Triển khai các hoạt động đào tạo bồi dưỡng, tập huấn chuyên sâu về kiến trúc, hạ tầng, dữ liệu, phân tích dữ liệu, sử dụng dữ liệu hỗ trợ ra quyết định và chỉ đạo điều hành của lãnh đạo các cấp; đào tạo nâng cao trình độ chuyên môn cho đội ngũ chuyên trách chuyển đổi số và an toàn, an ninh mạng	Các đơn vị phối hợp Bộ, ngành liên quan (nếu có)		

STT	Nội dung thực hiện	Đơn vị chủ trì	Đơn vị phối hợp	Thời gian hoàn thành
2.4	Cử cán bộ đại diện tham gia các Chương trình đào tạo, tập huấn đội ngũ chuyên gia Chính phủ điện tử, chuyên gia Chuyển đổi số; tham gia bồi dưỡng, tập huấn nâng cao năng lực, đáp ứng yêu cầu quản lý nhà nước và thực thi pháp luật về chuyển đổi số, phù hợp với tiêu chuẩn chức danh, vị trí việc làm	Các đơn vị phối hợp Bộ, ngành liên quan (nếu có)		
3	**Xây dựng, rà soát, sửa đổi quy định về bảo đảm an toàn, an ninh mạng phù hợp với các quy định về an toàn, an ninh mạng**			
3.1	Xây dựng Quy chế Bảo đảm an ninh mạng, an toàn thông tin tỉnh	Công an tỉnh	Các đơn vị liên quan	Quý IV năm 2025; Thường xuyên
3.2	Xây dựng phương án bảo đảm an toàn, an ninh mạng đối với hệ thống thông tin do tỉnh quản lý, bảo đảm đồng bộ, thống nhất, tập trung, có sự chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư trùng lặp	Công an tỉnh	Sở Khoa học và Công nghệ; các đơn vị liên quan	Quý IV năm 2025; Thường xuyên
3.3	Xây dựng, cập nhật quy định quản lý việc sử dụng máy tính nội bộ, máy tính có kết nối Internet, máy tính soạn thảo văn bản thuộc Danh mục bí mật nhà nước (đơn vị quy định cụ thể đối với yêu cầu quản lý, điều hành của đơn vị, phù hợp với quy định chung của tỉnh)	Các đơn vị trong tỉnh		Quý IV năm 2025; Thường xuyên
3.4	Xây dựng, cập nhật phương án bảo đảm an toàn, an ninh mạng đối với hệ thống thông tin do đơn vị quản lý thống nhất với phương án bảo đảm an toàn, an ninh mạng đối với hệ thống thông tin do các Bộ, ngành liên quan và tỉnh quản lý	Các đơn vị trong tỉnh		Quý IV năm 2025; Thường xuyên
3.5	Xây dựng, cập nhật quy định phương án ứng phó, khắc phục sự cố an toàn, an ninh mạng	Đội ứng cứu sự cố an toàn thông tin mạng		Quý IV năm 2025; Thường xuyên

STT	Nội dung thực hiện	Đơn vị chủ trì	Đơn vị phối hợp	Thời gian hoàn thành
3.6	Xây dựng phương án sao lưu, phục hồi dữ liệu, triển khai giải pháp để sẵng sàng phục hồi nhanh hoạt động của hệ thống thông tin khi gặp sự cố với chiến lược sao lưu dữ liệu theo nguyên tắc 3-2-1	Công an tỉnh; Đội ứng cứu sự cố an toàn thông tin mạng		Quý IV năm 2025; Thường xuyên
4	**Chỉ định, kiện toàn bộ phận/lực lượng thực hiện nhiệm vụ về an toàn, an ninh mạng**			
4.1	Xây dựng, trình cấp có thẩm quyền ban hành quyết định, quy định chức năng, nhiệm vụ của bộ phận thực hiện công tác bảo đảm an toàn, an ninh mạng cho hệ thống thông tin mà đơn vị quản lý, vận hành	Các đơn vị trong tỉnh		Quý IV năm 2025; Thường xuyên
4.2	Chỉ định cá nhân làm đầu mối phối hợp thực hiện công tác bảo đảm an toàn, an ninh mạng, bảo vệ dữ liệu cá nhân, ứng cứu sự cố tại đơn vị	Các đơn vị liên quan	Công an tỉnh	Quý IV năm 2025; Thường xuyên
4.3	Tiếp tục rà soát, kiện toàn tổ chức bộ máy, nhân lực của đơn vị chuyên trách về công nghệ thông tin, an toàn, an ninh mạng để tăng cường thực hiện nhiệm vụ, giải pháp mới về chuyển đổi số, tăng cường lực lượng bảo vệ an ninh mạng của tỉnh	Công an tỉnh	Sở Khoa học và Công nghệ; các đơn vị liên quan	Thường xuyên
5	**Xác định cấp độ an toàn hệ thống thông tin và triển khai phương án bảo đảm an toàn hệ thống thông tin theo cấp độ được phê duyệt**			
5.1	Rà soát, cập nhật và trình phê duyệt Hồ sơ đề xuất cấp độ hệ thống thông tin (bao gồm hệ thống có sử dụng camera giám sát)	Các đơn vị liên quan	Công an tỉnh; Văn phòng Tỉnh ủy	Quý IV năm 2025

STT	Nội dung thực hiện	Đơn vị chủ trì	Đơn vị phối hợp	Thời gian hoàn thành
5.2	Đề xuất nhiệm vụ/dự án để triển khai hoàn thiện phương án bảo đảm an toàn hệ thống thông tin theo cấp độ được phê duyệt	Các đơn vị liên quan	Công an tỉnh, Sở Tài chính; Văn phòng Tỉnh ủy	Thường xuyên
5.3	Báo cáo định kỳ của các đơn vị gửi Công an tỉnh	Các đơn vị liên quan	Công an tỉnh	Quý IV hàng năm
5.4	Báo cáo định kỳ của UBND tỉnh gửi Bộ Công an	Công an tỉnh		Quý IV hàng năm
6	**Triển khai bảo đảm an toàn thông tin theo mô hình 4 lớp**			
6.1	Tổ chức lực lượng tại chỗ: kiện toàn đơn vị đầu mối về an toàn thông tin mạng để làm tốt công tác tham mưu, 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	Công an tỉnh	Sở Khoa học và Công nghệ; các đơn vị liên quan	Thường xuyên
6.2	Thuê tổ chức, doanh nghiệp có đủ năng lực để thực hiện cung cấp dịch vụ giám sát, ứng cứu sự cố, bảo vệ an toàn thông tin mạng	Công an tỉnh	Sở Khoa học và Công nghệ	Thường xuyên
6.3	Thuê tổ chức, doanh nghiệp độc lập với tổ chức, doanh nghiệp giám sát/bảo vệ định kỳ kiểm tra, đánh giá an toàn thông tin mạng đối với hệ thống thông tin cấp độ 3 trở lên	Công an tỉnh	Sở Khoa học và Công nghệ	Hàng năm
6.4	Kết nối, chia sẻ thông tin giám sát với Trung tâm An ninh mạng quốc gia	Công an tỉnh	Sở Khoa học và Công nghệ	Thường xuyên
7	**Điều phối, diễn tập ứng cứu sự cố an toàn, an ninh mạng**			
7.1	Thành lập Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Quảng Trị	Công an tỉnh	Các đơn vị liên quan	Quý IV năm 2025

STT	Nội dung thực hiện	Đơn vị chủ trì	Đơn vị phối hợp	Thời gian hoàn thành
7.2	Tổ chức, tham gia diễn tập ứng cứu sự cố an toàn thông tin mạng đối với các hệ thống thông tin	Công an tỉnh; Đội ứng cứu sự cố an toàn thông tin mạng	Các đơn vị liên quan	Quý IV năm 2025; Hàng năm
7.3	Tổ chức diễn tập thực chiến trên hệ thống thông tin đang quản lý vận hành	Công an tỉnh; Đội ứng cứu sự cố an toàn thông tin mạng	Các đơn vị liên quan	Quý IV năm 2025; Hàng năm
7.4	Tổng hợp, xây dựng báo cáo định kỳ theo quy định	Đội Ứng cứu sự cố an toàn thông tin mạng	Các đơn vị liên quan	Quý IV năm 2025; Hàng năm
8	**Phòng chống mã độc tập trung và chia sẻ thông tin mã độc**			
8.1	Rà soát, thống kê tình hình sử dụng phần mềm bản quyền được cài đặt trên máy tính	Công an tỉnh	Các đơn vị liên quan	Hàng năm
8.2	Tiếp tục tổ chức triển khai hệ thống phòng chống mã độc cho các hệ thống thông tin	Các đơn vị liên quan	Công an tỉnh	Thường xuyên
8.3	Thực hiện chia sẻ thông tin mã độc cho hệ thống tổng hợp, chia sẻ thông tin mã độc của tỉnh	Các đơn vị liên quan	Công an tỉnh	Thường xuyên
8.4	Tổ chức tổng hợp, chia sẻ thông tin mã độc với hệ thống giám sát an ninh mạng quốc gia; hướng dẫn các đơn vị thực hiện	Công an tỉnh		Thường xuyên
9	**Giám sát và chia sẻ thông tin giám sát an toàn, an ninh mạng**			

STT	Nội dung thực hiện	Đơn vị chủ trì	Đơn vị phối hợp	Thời gian hoàn thành
9.1	Giám sát an toàn thông tin và kết nối, chia sẻ thông tin với Trung tâm An ninh mạng quốc gia	Công an tỉnh	Các đơn vị liên quan	Thường xuyên
9.2	Tham mưu trang cấp các thiết bị/giải pháp giám sát an toàn thông tin, kết nối, chia sẻ thông tin với Trung tâm An ninh mạng quốc gia	Công an tỉnh	Sở Khoa học và Công nghệ	Thường xuyên
9.3	Xây dựng Trung tâm An ninh mạng tỉnh Quảng Trị	Công an tỉnh	Sở Khoa học và Công nghệ; các đơn vị liên quan	Năm 2026
10	**Kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin do đơn vị quản lý, vận hành**	Công an tỉnh	Các đơn vị liên quan	- Định kỳ hàng năm kiểm tra, đánh giá đối với hệ thống cấp độ 3; hai năm một lần đối với các hệ thống thông tin cấp độ 1, cấp độ 2. - Công an tỉnh chủ trì kiểm tra, đánh giá các hệ thống thông tin cấp độ 2, cấp độ 3; các cơ quan, đơn vị chủ trì triển khai đối với hệ thống trong tổ chức mình
11	**Tạo lập niềm tin số, xây dựng môi trường mạng trung thực, văn minh, lành mạnh và phòng, chống vi phạm pháp luật trên không gian mạng**			
11.1	Giám sát, rà soát, phát hiện và thông báo, phối hợp với Bộ Công an, Bộ Khoa học và Công nghệ, doanh nghiệp nền tảng số xử lý, gỡ bỏ thông tin vi phạm pháp luật trên môi trường mạng	Công an tỉnh	Các đơn vị liên quan	Thường xuyên; theo quy định của pháp luật và hướng dẫn của Bộ Công an, Bộ Thông tin và Truyền thông

STT	Nội dung thực hiện	Đơn vị chủ trì	Đơn vị phối hợp	Thời gian hoàn thành
11.2	Phát triển các website, trang mạng xã hội, tài khoản trên môi trường mạng uy tín, nhiều tương tác để tuyên truyền định hướng thông tin, dư luận và phản bác hiệu quả các thông tin tiêu cực về đất nước, con người Việt Nam	Các đơn vị liên quan		Thường xuyên; theo quy định của pháp luật và hướng dẫn của Bộ Công an, Bộ Thông tin và Truyền thông
11.3	Dán nhãn tín nhiệm mạng cho các trang, cổng thông tin điện tử của cơ quan nhà nước trên địa bàn tỉnh	Các đơn vị liên quan	Công an tỉnh	Năm 2026
12	**Bảo vệ dữ liệu cá nhân**			
12.1	Xây dựng Quy chế Bảo vệ dữ liệu cá nhân	Công an tỉnh	Các đơn vị liên quan	Quý I năm 2026
12.2	Tham mưu UBND tỉnh, người đứng đầu các cơ quan chỉ định, phân công bộ phận, nhân sự có chức năng bảo vệ dữ liệu cá nhân trong đơn vị nhằm bảo đảm thực hiện quy định về bảo vệ dữ liệu cá nhân	Công an tỉnh; các đơn vị liên quan		Quý I năm 2026