

KẾ HOẠCH

Triển khai thực hiện Đề án "Nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng quốc gia" trên địa bàn tỉnh Thanh Hóa

Thực hiện Quyết định số 515/QĐ-TTg ngày 30/3/2026 của Thủ tướng Chính phủ (sau đây gọi tắt là Quyết định số 515/QĐ-TTg) về việc phê duyệt Đề án "Nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng quốc gia" (Đề án), UBND tỉnh ban hành kế hoạch triển khai thực hiện, cụ thể như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Tổ chức quán triệt, triển khai thực hiện Quyết định số 515/QĐ-TTg; chủ động thực hiện các giải pháp góp phần nâng cao năng lực của lực lượng bảo vệ an ninh mạng của tỉnh theo hướng tinh nhuệ, hiện đại.

- Tăng cường hoạt động của lực lượng bảo vệ an ninh mạng, Đội ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh theo hướng cách mạng, chính quy, tinh nhuệ, hiện đại. Phối hợp đồng bộ, thống nhất, hiệu quả giữa các lực lượng, xây dựng thể trận an ninh nhân dân trên không gian mạng, huy động sức mạnh tổng hợp của cả hệ thống chính trị và toàn dân trong bảo vệ chủ quyền quốc gia trên không gian mạng.

- Thiết lập hệ thống phòng thủ chuyên sâu để bảo vệ tuyệt đối an toàn các hệ thống thông tin trọng yếu của Đảng và Nhà nước trên địa bàn tỉnh. Hình thành lực lượng chuyên trách tinh nhuệ đảm bảo khả năng sẵn sàng, chủ động ứng phó, không để bị động, bất ngờ trước các nguy cơ, thách thức trên không gian mạng.

2. Yêu cầu

- Việc tổ chức triển khai thực hiện Quyết định số 515/QĐ-TTg phải thực hiện nghiêm túc, quyết liệt, hiệu quả, đồng bộ từ tỉnh đến cơ sở; tập trung thực hiện những nhiệm vụ trọng tâm, trọng điểm nhằm nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng; xác định rõ từng nhiệm vụ cụ thể, thời gian, lộ trình, điều kiện đảm bảo.

- Xác định rõ trách nhiệm của người đứng đầu đơn vị, địa phương trong công tác bảo đảm an ninh mạng; coi đây là nhiệm vụ trọng tâm, thường xuyên, trực tiếp lãnh đạo, chỉ đạo và chịu trách nhiệm toàn diện trước UBND tỉnh nếu để xảy ra mất an toàn, an ninh mạng thuộc phạm vi quản lý.

- Các sở, ban, ngành, đơn vị cấp tỉnh, UBND các xã, phường đẩy mạnh công tác tuyên truyền, phổ biến sâu rộng mục tiêu, lộ trình của Đề án; khuyến khích Nhân dân, cộng đồng doanh nghiệp, đội ngũ tri thức tích cực xây dựng phong trào nghiên cứu, phát triển khoa học công nghệ, đổi mới sáng tạo và chuyển đổi số, đặc biệt là các sản phẩm công nghệ đảm bảo an ninh mạng, mang tính chiến lược “Make in Vietnam”.

- Huy động và sử dụng có hiệu quả, tiết kiệm các nguồn lực nhất là nguồn ngân sách nhà nước, ưu tiên đầu tư cho phát triển khoa học công nghệ, chuyển đổi số bảo đảm công khai và minh bạch trong việc huy động và sử dụng.

II. MỤC TIÊU

1. Mục tiêu chung

Nâng cao năng lực tổng thể, xây dựng lực lượng bảo vệ an ninh mạng tinh nhuệ, hiện đại, nhằm chủ động phòng ngừa, sẵn sàng ứng phó hiệu quả với mọi nguy cơ, thách thức trên không gian mạng, bảo vệ vững chắc an ninh quốc gia, trật tự an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân trên không gian mạng.

2. Mục tiêu đến năm 2030

a) Nguồn lực đảm bảo an ninh mạng

- Phấn đấu đến năm 2030, tỉnh Thanh Hoá cơ bản đảm bảo đủ nhu cầu số lượng chuyên gia an ninh mạng chuyên sâu, trong đó có 20% đạt trình độ quốc gia, quốc tế.

- Đạt 100% lực lượng chuyên trách bảo vệ an ninh mạng của tỉnh, cán bộ trực tiếp quản trị hệ thống thông tin cấp độ 3, cấp độ 4, cấp độ 5 trong cơ quan, tổ chức, doanh nghiệp nhà nước trên địa bàn tỉnh có chứng nhận đáp ứng yêu cầu kiến thức, kỹ năng chuyên sâu về an ninh mạng do cơ quan có thẩm quyền cấp; được cập nhật kiến thức an ninh mạng ít nhất 01 lần/năm.

- Đạt 90% người sử dụng Internet có cơ hội tiếp cận hoạt động nâng cao nhận thức, kỹ năng và công cụ bảo đảm an ninh mạng.

b) Cơ sở hạ tầng đảm bảo an ninh mạng

- Đạt 100% các hệ thống thông tin sử dụng vốn ngân sách nhà nước trên địa bàn tỉnh được triển khai đầy đủ các phương án bảo đảm an ninh mạng theo cấp độ.

- Đạt 70% hệ thống thông tin quan trọng trên địa bàn tỉnh sử dụng sản phẩm công nghệ chiến lược “Make in Vietnam”; 100% các sản phẩm, dịch vụ an ninh mạng phải được kiểm định, đánh giá trước khi đưa vào sử dụng, áp dụng trước hết với hạ tầng thông tin quan trọng của tỉnh có ảnh hưởng trực tiếp đến an ninh quốc gia, trật tự xã hội và đời sống nhân dân.

c) Đào tạo lực lượng đảm bảo an ninh mạng

- Phổ biến, áp dụng chuẩn kiến thức, kỹ năng chuyên sâu, chương trình, nội dung tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng; quản lý, hướng dẫn và tổ chức triển khai hoạt động chứng nhận tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng theo hướng dẫn của các bộ, ngành trung ương.

- Mỗi năm, căn cứ theo tình hình thực tế, cử ít nhất 50 cán bộ lực lượng bảo vệ an ninh mạng của tỉnh tham gia huấn luyện tại các cơ sở đào tạo/huấn luyện an ninh mạng uy tín cả trong và ngoài nước. Hình thành và phát triển đội ngũ cán bộ chuyên trách về an ninh mạng chất lượng cao.

d) Nâng cao năng lực tự chủ an ninh mạng

- Nghiên cứu, phát triển, làm chủ công nghệ chiến lược về an ninh mạng. Xây dựng, phát triển hệ sinh thái sản phẩm, dịch vụ an ninh mạng do Việt Nam làm chủ công nghệ. Lựa chọn tối thiểu 02 tổ chức, doanh nghiệp của tỉnh có khả năng làm chủ công nghệ cho mỗi loại sản phẩm, dịch vụ an ninh mạng trọng điểm, nền tảng để tập trung nguồn lực thúc đẩy.

- Nghiên cứu thu hút ít nhất 01 doanh nghiệp về an ninh mạng nước ngoài có quy mô lớn đặt trung tâm nghiên cứu và phát triển tại địa phương.

e) Hợp tác đảm bảo an ninh mạng

- Phối hợp với lực lượng bảo vệ an ninh mạng và các doanh nghiệp an ninh mạng trong cả nước để chia sẻ thông tin, cảnh báo, điều phối ứng phó sự cố nhằm nâng cao năng lực phòng thủ quốc gia.

- Tham gia tích cực hoạt động của các tổ chức uy tín về an ninh mạng, thiết lập, duy trì kết nối với các lực lượng đảm bảo an ninh mạng trong và ngoài nước. Thiết lập đường dây nóng 24/7 cho các lực lượng tham gia ứng cứu khẩn cấp sự cố an ninh mạng trên địa bàn tỉnh.

3. Tầm nhìn đến 2045

Phấn đấu đưa tỉnh Thanh Hoá trở thành tỉnh nằm trong nhóm 10 địa phương dẫn đầu cả nước về an ninh mạng, có năng lực mạnh trong phòng thủ, tấn công, trấn áp tội phạm mạng và các thế lực thù địch, bảo vệ vững chắc chủ quyền số, bảo vệ cho mọi hoạt động của chính quyền, doanh nghiệp và người dân trên không gian mạng. Đưa công nghiệp an ninh mạng trở thành ngành kinh tế mũi nhọn, có từ 02 doanh nghiệp an ninh mạng của tỉnh vươn tầm quốc tế, nằm trong nhóm các doanh nghiệp dẫn đầu cả nước về cung cấp giải pháp an ninh mạng, dịch vụ, công nghệ.

III. NHIỆM VỤ, GIẢI PHÁP

1. Tuyên truyền, phổ biến các văn bản quy phạm pháp luật; tập huấn, nâng cao nhận thức, kỹ năng về an ninh mạng

- Thủ trưởng, người đứng đầu các cơ quan, đơn vị trên địa bàn tỉnh căn cứ tình hình thực tế để tiến hành tổ chức quán triệt nghiêm túc Quyết định số 515/QĐ-

TTg ngày 30/3/2026 của Thủ tướng Chính phủ phê duyệt Đề án “Nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng quốc gia”; Luật An ninh mạng số 116/2025/QH15 và các quy định về công tác bảo đảm an ninh mạng.

Đơn vị chủ trì: Các sở, ban, ngành, đơn vị cấp tỉnh, UBND các xã, phường.

Thời gian thực hiện: Hoàn thành trước ngày 05/6/2026.

- Đổi mới nội dung, đa dạng hóa hình thức tuyên truyền theo hướng thiết thực, hiệu quả; tăng cường ứng dụng công nghệ số, nền tảng trực tuyến, hệ thống thông tin cơ sở để nâng cao phạm vi tiếp cận và chất lượng tuyên truyền.

Đơn vị chủ trì: Các sở, ban, ngành, đơn vị cấp tỉnh, UBND các xã, phường.

Thời gian thực hiện: Thường xuyên.

- Xây dựng, cập nhật, bổ sung nội dung chương trình đào tạo kỹ năng số (bảo đảm an ninh mạng, quản trị dữ liệu, sử dụng nền tảng số,..) cho lãnh đạo các đơn vị; định kỳ tổ chức các lớp tập huấn, bồi dưỡng kiến thức về an ninh mạng, chuyển đổi số, kỹ năng số cho cán bộ, công chức, viên chức, nhất là trong hoạt động hành chính công. Tích hợp, lồng ghép nội dung chuyển đổi số, đổi mới sáng tạo trong chương trình đào tạo chính quy, bồi dưỡng cán bộ; liên kết với các tổ chức, doanh nghiệp công nghệ để xây dựng chương trình thực hành, trao đổi chuyên môn,..., trong đó:

+ Tổ chức tập huấn chuyên sâu cho đội ngũ cán bộ lãnh đạo, quản lý nhằm nâng cao nhận thức, năng lực chỉ đạo, điều hành trong công tác bảo đảm an ninh mạng;

+ Tập huấn nghiệp vụ cho cán bộ chuyên trách, bán chuyên trách về an toàn thông tin, an ninh mạng, tập trung vào kỹ năng quản trị hệ thống, giám sát, phát hiện, xử lý sự cố, ứng cứu khẩn cấp;

+ Tập huấn, hướng dẫn kỹ năng cơ bản cho cán bộ, công chức, viên chức và người lao động trong việc sử dụng hệ thống thông tin an toàn, phòng tránh các nguy cơ mất an ninh mạng (lừa đảo trực tuyến, mã độc, rò rỉ dữ liệu...).

Đơn vị chủ trì: Công an tỉnh.

Đơn vị phối hợp: Sở Nội vụ và các đơn vị có liên quan.

Thời gian thực hiện: Hằng năm.

- Tổ chức các hội nghị, hội thảo, diễn tập thực hành về an ninh mạng, an toàn thông tin; lồng ghép nội dung diễn tập ứng cứu sự cố vào chương trình tập huấn nhằm nâng cao kỹ năng thực tiễn, khả năng phối hợp xử lý tình huống.

Đơn vị chủ trì: Công an tỉnh.

Đơn vị phối hợp: Các sở, ban, ngành, đơn vị cấp tỉnh, UBND các xã, phường và các đơn vị có liên quan.

Thời gian thực hiện: Hằng năm.

2. Hoàn thiện cơ chế, chính sách

a) Rà soát, hoàn thiện hệ thống văn bản quy phạm pháp luật và quy định nội bộ

- Thường xuyên tổ chức rà soát toàn diện các văn bản quy phạm pháp luật, quy chế, quy định nội bộ của tỉnh liên quan đến công tác bảo đảm an ninh mạng để kịp thời sửa đổi, bổ sung hoặc ban hành mới bảo đảm phù hợp với quy định của pháp luật hiện hành và yêu cầu thực tiễn.

Đơn vị chủ trì: Công an tỉnh.

Đơn vị phối hợp: Sở Khoa học và Công nghệ, Sở Tư pháp và các đơn vị có liên quan.

Thời gian thực hiện: Thường xuyên.

- Xây dựng, ban hành các quy chế quản lý, vận hành, khai thác và bảo đảm an ninh mạng đối với các hệ thống thông tin, cơ sở dữ liệu thuộc phạm vi quản lý của UBND tỉnh; quy định rõ trách nhiệm của từng cơ quan, đơn vị, cá nhân.

Đơn vị chủ trì: Đơn vị chủ quản, vận hành hệ thống thông tin (các sở, ban, ngành, địa phương).

Thời gian thực hiện: Hoàn thành trong tháng 6/2026.

- Chuẩn hóa quy trình quản lý rủi ro, kiểm tra, đánh giá an toàn thông tin, phân loại cấp độ an toàn hệ thống thông tin theo hướng dẫn của các bộ, ngành trung ương.

Đơn vị chủ trì: Công an tỉnh.

Đơn vị phối hợp: Các sở, ban, ngành, đơn vị cấp tỉnh, UBND các xã, phường.

Thời gian thực hiện: Thực hiện ngay sau khi có hướng dẫn của các bộ, ngành Trung ương.

- Nghiên cứu, tổ chức triển khai có hiệu quả các cơ chế và chính sách ưu đãi nhằm thu hút, trọng dụng, bồi dưỡng, nâng cao chất lượng nguồn nhân lực cho lực lượng bảo vệ an ninh mạng trên địa bàn tỉnh theo quy định của pháp luật hiện hành và hướng dẫn của cơ quan có thẩm quyền.

Đơn vị chủ trì: Sở Nội vụ.

Đơn vị phối hợp: Công an tỉnh, Sở Khoa học và Công nghệ, Sở Tài chính và các đơn vị có liên quan.

Thời gian thực hiện: Thực hiện ngay sau khi có hướng dẫn của các bộ, ngành Trung ương.

b) Xây dựng và hoàn thiện cơ chế phối hợp liên ngành

- Xây dựng quy chế phối hợp liên ngành giữa các cơ quan, đơn vị, địa phương và các lực lượng chức năng trong công tác bảo đảm an ninh mạng, phòng ngừa, phát hiện và xử lý sự cố an ninh mạng. Quy định cụ thể đầu mối, trách

nhệm phối hợp, chế độ trao đổi, chia sẻ thông tin, cảnh báo sớm và hỗ trợ ứng cứu sự cố giữa các cơ quan, đơn vị.

Đơn vị chủ trì: Đơn vị chủ quản, vận hành hệ thống thông tin (các sở, ban, ngành, địa phương).

Thời gian thực hiện: Thực hiện ngay sau khi có hướng dẫn của các bộ, ngành Trung ương.

- Thiết lập cơ chế phối hợp với các bộ, ngành Trung ương, doanh nghiệp cung cấp dịch vụ công nghệ thông tin, viễn thông trong công tác bảo đảm an ninh mạng trên địa bàn tỉnh.

Đơn vị chủ trì: Công an tỉnh.

Đơn vị phối hợp: Các sở, ban, ngành, đơn vị cấp tỉnh, UBND các xã, phường.

Thời gian thực hiện: Thực hiện ngay sau khi có hướng dẫn của các bộ, ngành Trung ương..

3. Đảm bảo an ninh mạng đối với hệ thống thông tin trên địa bàn tỉnh

a) Hoàn thiện, triển khai hồ sơ đề xuất cấp độ an toàn hệ thống thông tin

- Yêu cầu 100% hệ thống thông tin do UBND tỉnh chủ quản đang vận hành phải có hồ sơ đề xuất cấp độ được phê duyệt đảm bảo theo quy định của pháp luật¹. Triển khai phương án đảm bảo an ninh mạng theo hồ sơ đề xuất cấp độ an toàn hệ thống thông tin được đơn vị có thẩm quyền phê duyệt; khắc phục tình trạng “nợ tuân thủ”.

Đơn vị chủ trì: Công an tỉnh.

Đơn vị phối hợp: Đơn vị chủ quản, vận hành hệ thống thông tin (các sở, ban, ngành, địa phương) và các đơn vị liên quan.

Thời gian thực hiện: Hoàn thành trong tháng 6/2026.

b) Đầu tư, triển khai cơ sở hạ tầng đảm bảo an ninh mạng

- Xây dựng, mở rộng hệ thống Giám sát an toàn thông tin mạng (SOC) thực hiện giám sát, bảo đảm an toàn thông tin mạng cho toàn bộ các cơ quan trong hệ thống chính trị tại địa phương, kết nối Trung tâm an ninh mạng quốc gia.

Đơn vị chủ trì: Công an tỉnh.

Đơn vị phối hợp: Sở Tài chính, Sở Khoa học và Công nghệ.

Thời gian thực hiện: Trong tháng 6/2026 hoàn thiện hồ sơ trình UBND tỉnh ban hành Quyết định phê duyệt chủ trương đầu tư.

- Các cơ quan, đơn vị trên địa bàn tỉnh chủ động khảo sát nhu cầu trang thiết bị, phần mềm phục vụ công tác đảm bảo an ninh mạng. Xây dựng các phương án đầu tư, nâng cấp hạ tầng kỹ thuật đảm bảo đồng bộ từ trung ương đến địa

¹ Theo Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19/11/2015; Luật An ninh mạng ngày 12/6/2018; 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.

phương. Ưu tiên sử dụng các sản phẩm công nghệ chiến lược “Make in Vietnam” cho các hệ thống thông tin trên địa bàn tỉnh.

Đơn vị chủ trì: Đơn vị chủ quản, quản lý, vận hành hệ thống thông tin (các sở, ban, ngành, địa phương).

Đơn vị phối hợp: Sở Tài chính, Sở Khoa học và Công nghệ.

Thời gian thực hiện: Hằng năm.

c) Định kỳ đánh giá các nguy cơ, sự cố an toàn thông tin mạng

- Kiểm định, đánh giá các sản phẩm, dịch vụ an ninh mạng trước khi đưa vào sử dụng đối với hạ tầng thông tin quan trọng, hệ thống thông tin của các cơ quan trong hệ thống chính trị có ảnh hưởng trực tiếp đến an ninh quốc gia, trật tự xã hội và đời sống Nhân dân.

Đơn vị chủ trì: Đơn vị chủ quản, quản lý, vận hành hệ thống thông tin (các sở, ban, ngành, địa phương).

Đơn vị phối hợp: Công an tỉnh, Sở Khoa học và Công nghệ.

Thời gian thực hiện: Hoàn thành trong tháng 6/2026.

- Tổ chức đánh giá hiện trạng và khả năng bảo đảm an toàn thông tin mạng đối với hệ thống thông tin; đánh giá, dự báo các nguy cơ, sự cố hệ thống thông tin có thể xảy ra; dự báo đối tượng có thể tấn công, phá hoại gây ra sự cố mất an toàn thông tin mạng; đánh giá, dự báo các hậu quả, thiệt hại, tác động gây ra nếu xảy ra sự cố; đánh giá về hiện trạng phương tiện, trang thiết bị, công cụ hỗ trợ, nhân lực phục vụ công tác ứng phó, ứng cứu, khắc phục sự cố của cơ quan, đơn vị (bao gồm của cả nhà thầu đã ký hợp đồng cung cấp dịch vụ nếu có).

Đơn vị chủ trì: Đơn vị chủ quản, quản lý, vận hành hệ thống thông tin (các sở, ban, ngành, địa phương).

Đơn vị phối hợp: Công an tỉnh, Sở Khoa học và Công nghệ.

Thời gian thực hiện: Hoàn thành trong tháng 6/2026.

- Chủ động thực hiện sẵn lòng môi nguy hại và rà quét lỗ hổng bảo mật đối với các hệ thống thông tin thuộc phạm vi quản lý; khắc phục lỗ hổng, điểm yếu theo cảnh báo của cơ quan chức năng.

Đơn vị chủ trì: Đơn vị chủ quản, quản lý, vận hành hệ thống thông tin (các sở, ban, ngành, địa phương); các đơn vị có liên quan.

Đơn vị phối hợp: Công an tỉnh, Sở Khoa học và Công nghệ.

Thời gian thực hiện: Thường xuyên.

4. Giám sát, chia sẻ thông tin và đánh giá năng lực an ninh mạng

- Xây dựng, vận hành hệ thống giám sát, điều hành an toàn thông tin mạng của tỉnh theo hướng tập trung, liên thông, kết nối với hệ thống giám sát quốc gia. Thiết lập cơ chế thu thập, phân tích, xử lý, chia sẻ thông tin về nguy cơ, sự cố an

ninh mạng giữa các cơ quan, đơn vị, địa phương và với các cơ quan Trung ương.

Đơn vị chủ trì: Công an tỉnh.

Đơn vị phối hợp: Sở Khoa học và Công nghệ và các đơn vị có liên quan.

Thời gian thực hiện: Thực hiện theo hướng dẫn của các bộ, ngành Trung ương.

- Tổ chức theo dõi, giám sát thường xuyên tình trạng an toàn thông tin của các hệ thống; kịp thời cảnh báo, hướng dẫn xử lý các nguy cơ mất an ninh mạng. Thực hiện đánh giá định kỳ, đột xuất về năng lực bảo đảm an ninh mạng của các cơ quan, đơn vị; công bố, xếp hạng mức độ an ninh mạng theo hướng dẫn của các bộ, ngành trung ương.

Đơn vị chủ trì: Công an tỉnh.

Đơn vị phối hợp: Các sở, ban, ngành, đơn vị cấp tỉnh, UBND các xã, phường.

Thời gian thực hiện: Thực hiện theo hướng dẫn của các bộ, ngành Trung ương.

- Xây dựng cơ sở dữ liệu, hệ thống báo cáo, thống kê về an ninh mạng phục vụ công tác chỉ đạo, điều hành; ứng dụng công nghệ số trong quản lý, giám sát, đánh giá.

Đơn vị chủ trì: Công an tỉnh.

Đơn vị phối hợp: Sở Khoa học và Công nghệ.

Thời gian thực hiện: Thực hiện theo hướng dẫn của các bộ, ngành Trung ương.

5. Tổ chức, phát triển lực lượng an ninh mạng

a) Xây dựng, tổ chức lực lượng an ninh mạng

- củng cố, kiện toàn Tiểu ban An ninh mạng tỉnh Thanh Hoá.

Đơn vị chủ trì: Công an tỉnh.

Đơn vị phối hợp: Các sở, ban, ngành, đơn vị cấp tỉnh.

Thời gian thực hiện: Khi có sự thay đổi về thành viên tham gia.

- Xây dựng, kiện toàn Đội Ứng cứu sự cố an ninh mạng tỉnh Thanh Hoá.

Đơn vị chủ trì: Công an tỉnh.

Đơn vị phối hợp: Các sở, ban, ngành, đơn vị cấp tỉnh, UBND xã, phường và các đơn vị có liên quan.

Thời gian thực hiện: Hoàn thành trước ngày 05/6/2026.

b) Phát triển nguồn nhân lực thực hiện công tác đảm bảo an ninh mạng

- Rà soát vị trí việc làm, đội ngũ cán bộ chuyên trách an ninh mạng; đánh giá năng lực, trình độ, số lượng đáp ứng yêu cầu trên phạm vi toàn tỉnh.

Đơn vị chủ trì: Công an tỉnh.

Đơn vị phối hợp: Các sở, ban, ngành, đơn vị cấp tỉnh, UBND các xã, phường và các đơn vị có liên quan.

Thời gian thực hiện: Thực hiện ngay sau khi có hướng dẫn của các bộ, ngành Trung ương.

- Xây dựng, ban hành và định kỳ cập nhật khung đánh giá năng lực vị trí việc làm đối với cán bộ thực hiện công tác đảm bảo an ninh mạng theo hướng dẫn của đơn vị cấp trên.

Đơn vị chủ trì: Sở Nội vụ.

Đơn vị phối hợp: Công an tỉnh; các sở, ban, ngành, đơn vị cấp tỉnh, UBND các xã, phường và các đơn vị có liên quan.

Thời gian thực hiện: Thực hiện ngay sau khi có hướng dẫn của các bộ, ngành Trung ương.

- Phổ biến, nâng cao kiến thức an ninh mạng cho người dân qua các nền tảng học tập số, “Bình dân học vụ số”, các khoá học trực tuyến đại chúng mở (MOOC) và các chiến dịch truyền thông đại chúng.

Đơn vị chủ trì: Công an tỉnh.

Đơn vị phối hợp: Các sở, ban, ngành, đơn vị cấp tỉnh, UBND các xã, phường và các đơn vị có liên quan.

Thời gian thực hiện: Thường xuyên.

- Phối hợp, lồng ghép đưa kiến thức về an ninh mạng đến với học sinh từ trung học cơ sở đến đại học; tổ chức các cuộc thi, diễn đàn, câu lạc bộ an ninh mạng học đường và duy trì hoạt động hằng năm.

Đơn vị chủ trì: Sở Giáo dục và Đào tạo.

Đơn vị phối hợp: Công an tỉnh, Sở Khoa học và Công nghệ.

Thời gian thực hiện: Thường xuyên.

c) Đào tạo, phát triển nguồn nhân lực an ninh mạng chất lượng cao

- Tham mưu cho UBND tỉnh tổ chức triển khai áp dụng tiêu chuẩn chức danh, vị trí việc làm, khung kiến thức, kỹ năng chuyên sâu về an ninh mạng; quy định về đào tạo, sát hạch, cấp chứng nhận đáp ứng yêu cầu về kiến thức, kỹ năng chuyên sâu về an ninh mạng cho lực lượng bảo vệ an ninh mạng, cán bộ trực tiếp quản trị vận hành hệ thống thông tin cấp độ 3, cấp độ 4, cấp độ 5 trong cơ quan, tổ chức, doanh nghiệp Nhà nước theo hướng dẫn của Bộ Công an và các bộ, ngành trung ương.

Đơn vị chủ trì: Công an tỉnh.

Đơn vị phối hợp: Sở Nội vụ, Sở Khoa học và Công nghệ.

Thời gian thực hiện: Thực hiện ngay sau khi có hướng dẫn của Bộ Công an và các bộ, ngành Trung ương.

- Hằng năm, trên cơ sở khảo sát nhu cầu thực tiễn, tổ chức các khoá đào tạo, tập huấn ngắn hạn theo hình thức tập trung, trực tuyến hoặc kết hợp cho các

cơ quan, đơn vị trên địa bàn tỉnh để cập nhật kiến thức, huấn luyện chuyên sâu kiến thức, kỹ năng an ninh mạng.

Đơn vị chủ trì: Sở Nội vụ.

Đơn vị phối hợp: Công an tỉnh, Sở Khoa học và Công nghệ; các sở, ban, ngành, đơn vị cấp tỉnh, UBND các xã, phường và các đơn vị có liên quan.

Thời gian thực hiện: Hằng năm.

- Hằng năm phối hợp với các tổ chức, doanh nghiệp và các đơn vị nhà nước có liên quan tổ chức ít nhất 01 chương trình diễn tập cấp tỉnh nhằm nâng cao năng lực ứng phó và phối hợp tác chiến trên không gian mạng.

Đơn vị chủ trì: Công an tỉnh.

Đơn vị phối hợp: Sở Khoa học và Công nghệ; các sở, ban, ngành, đơn vị cấp tỉnh, UBND các xã, phường và các đơn vị có liên quan.

Thời gian thực hiện: Hằng năm.

- Thúc đẩy hợp tác với các trường đại học, viện nghiên cứu uy tín trong và ngoài nước để đào tạo nguồn nhân lực chất lượng cao; đổi mới chương trình đào tạo, hiện đại hoá phương thức đào tạo và ứng dụng công nghệ tiên tiến nhất là điện toán đám mây, trí tuệ nhân tạo,... tạo điều kiện cho các sinh viên, giảng viên thực tập, nghiên cứu tại các doanh nghiệp.

Đơn vị chủ trì: Trường Đại học Hồng Đức.

Đơn vị phối hợp: Sở Ngoại vụ và các đơn vị có liên quan.

Thời gian thực hiện: Thường xuyên.

6. Nghiên cứu phát triển, nâng cao năng lực tự chủ công nghệ trong lĩnh vực an ninh mạng

a) Khuyến khích doanh nghiệp khởi nghiệp sáng tạo về an ninh mạng, công nghệ cao

- Tham mưu, xây dựng chính sách đột phá nhằm khuyến khích và thúc đẩy các doanh nghiệp khởi nghiệp sáng tạo về an ninh mạng; thu hút các doanh nghiệp trong và ngoài nước khởi nghiệp tại tỉnh Thanh Hoá, nhất là trong việc bảo đảm an ninh mạng, lĩnh vực khoa học, công nghệ và chuyển đổi số. Hỗ trợ các doanh nghiệp vừa và nhỏ bảo đảm an ninh mạng thông qua các gói hỗ trợ đào tạo, tư vấn, cung cấp giải pháp an ninh mạng nội địa.

Đơn vị chủ trì: Sở Khoa học và Công nghệ.

Đơn vị phối hợp: Sở Tài chính và các đơn vị có liên quan.

Thời gian thực hiện: Thường xuyên.

- Tăng cường hỗ trợ thủ tục pháp lý, văn phòng làm việc, đào tạo kỹ năng quản trị, marketing, gọi vốn,...; kết nối quỹ đầu tư, nhà đầu tư, cộng đồng cổ vấn cho các dự án khởi nghiệp của tỉnh. Cung cấp các ưu đãi, hỗ trợ các doanh nghiệp

chuyên về nghiên cứu và phát triển sản phẩm, dịch vụ an ninh mạng. Tổ chức các cuộc thi, giải thưởng nhằm tìm kiếm, đánh giá và công nhận các sản phẩm, dịch vụ an ninh mạng xuất sắc, chất lượng cao của các doanh nghiệp trong và ngoài tỉnh.

Đơn vị chủ trì: Sở Khoa học và Công nghệ.

Đơn vị phối hợp: Công an tỉnh và các đơn vị có liên quan.

Thời gian thực hiện: Thường xuyên.

b) Nâng cao năng lực nghiên cứu

- Ưu tiên nghiên cứu, phát triển các sản phẩm công nghệ về an ninh mạng, chuyển đổi số đặc biệt các sản phẩm công nghệ lõi mang tính chiến lược “Make in Vietnam”.

Đơn vị chủ trì: Sở Khoa học và Công nghệ.

Đơn vị phối hợp: Công an tỉnh; các sở, ban, ngành, đơn vị cấp tỉnh, UBND các xã, phường và các đơn vị có liên quan.

Thời gian thực hiện: Thường xuyên.

- Tăng cường phối hợp với các trường đại học, viện nghiên cứu trong và ngoài nước; thúc đẩy, khuyến khích các nhà khoa học nghiên cứu và công bố công trình khoa học, đăng ký bảo hộ quyền sở hữu trí tuệ.

Đơn vị chủ trì: Trường Đại học Hồng Đức.

Đơn vị phối hợp: Sở Ngoại vụ và các đơn vị có liên quan.

Thời gian thực hiện: Thường xuyên.

- Tăng cường phối hợp công tư, xây dựng và vận hành có hiệu quả mối quan hệ Nhà nước - Nhà trường (Viện nghiên cứu) - Doanh nghiệp trong việc định hướng, nghiên cứu, nắm bắt các công nghệ lõi, công nghệ chiến lược, phát triển, triển khai các công nghệ, sản phẩm, dịch vụ an ninh mạng.

Đơn vị chủ trì: Sở Khoa học và Công nghệ.

Đơn vị phối hợp: Sở Tài chính, Trường Đại học Hồng Đức.

Thời gian thực hiện: Thường xuyên.

7. Tăng cường hợp tác quốc tế trong lĩnh vực an ninh mạng

- Triển khai các hoạt động hợp tác quốc tế về an ninh mạng phù hợp với chủ trương, chính sách của Đảng, pháp luật của Nhà nước và định hướng đối ngoại của tỉnh.

Đơn vị chủ trì: Công an tỉnh.

Đơn vị phối hợp: Sở Khoa học và Công nghệ, Sở Ngoại vụ và các đơn vị liên quan.

Thời gian thực hiện: Thường xuyên.

- Thiết lập, duy trì quan hệ hợp tác với các tổ chức quốc tế, cơ quan đại diện ngoại giao, doanh nghiệp công nghệ nhằm trao đổi thông tin, chia sẻ kinh nghiệm, tiếp nhận hỗ trợ kỹ thuật và chuyển giao công nghệ.

Đơn vị chủ trì: Sở Khoa học và Công nghệ.

Đơn vị phối hợp: Công an tỉnh, Sở Ngoại vụ và các đơn vị liên quan.

Thời gian thực hiện: Thường xuyên.

- Tham gia, phối hợp tổ chức các hội nghị, hội thảo, chương trình đào tạo có yếu tố nước ngoài; cập nhật xu hướng, giải pháp mới về an ninh mạng phục vụ công tác tại địa phương. Tiếp nhận, triển khai hiệu quả các chương trình, dự án hợp tác quốc tế về đào tạo nguồn nhân lực, nâng cao năng lực bảo đảm an ninh mạng. Tăng cường trao đổi, chia sẻ thông tin về nguy cơ, sự cố an ninh mạng có yếu tố nước ngoài; phối hợp cảnh báo, phòng ngừa, xử lý theo quy định. Quản lý chặt chẽ các hoạt động hợp tác quốc tế trong lĩnh vực an ninh mạng; bảo đảm tuân thủ quy định pháp luật, không để phát sinh yếu tố phức tạp về an ninh, trật tự.

Đơn vị chủ trì: Công an tỉnh

Đơn vị phối hợp: Sở Khoa học và Công nghệ, Sở Ngoại vụ và các đơn vị có liên quan.

Thời gian thực hiện: Thường xuyên.

IV. KINH PHÍ THỰC HIỆN

- Kinh phí thực hiện Kế hoạch này được bố trí từ nguồn ngân sách chi cho hoạt động khoa học, công nghệ, đổi mới sáng tạo, nguồn xã hội hoá và các nguồn hợp pháp khác theo quy định của pháp luật.

- Xây dựng cơ chế linh hoạt, minh bạch, công khai trong quản lý, sử dụng kinh phí; tăng cường kiểm tra, giám sát, tránh tiêu cực, lãng phí.

V. TỔ CHỨC THỰC HIỆN

1. Việc triển khai thực hiện các nhiệm vụ của Kế hoạch được thực hiện trên cơ sở tận dụng hạ tầng kỹ thuật, cơ sở vật chất, trang thiết bị và nguồn nhân lực hiện có; lồng ghép với các chương trình, đề án, kế hoạch có liên quan nhằm bảo đảm tính khả thi, hiệu quả và phù hợp với khả năng cân đối nguồn lực của tỉnh. Quá trình tổ chức thực hiện được triển khai linh hoạt theo yêu cầu thực tiễn, mức độ cấp thiết của từng nhiệm vụ và hướng dẫn của các bộ, ngành trung ương; bảo đảm chủ động rà soát, điều chỉnh phù hợp với tình hình thực tế trong từng thời kỳ.

2. Các sở, ban, ngành, đơn vị cấp tỉnh và UBND các xã, phường, căn cứ chức năng, nhiệm vụ được giao, có trách nhiệm tổ chức triển khai thực hiện nghiêm túc, đồng bộ và hiệu quả các nội dung của Kế hoạch này; xây dựng kế hoạch cụ thể của cơ quan, đơn vị mình, bảo đảm phù hợp với tình hình thực tiễn,

không chồng chéo, trùng lặp với các chương trình, đề án, kế hoạch về chuyển đổi số, ứng dụng công nghệ thông tin và bảo đảm an ninh mạng đã và đang triển khai.

3. Thủ trưởng, người đứng đầu các cơ quan, đơn vị chịu trách nhiệm toàn diện trước Chủ tịch UBND tỉnh về kết quả triển khai thực hiện công tác bảo đảm an ninh mạng tại cơ quan, đơn vị mình; trực tiếp chỉ đạo, phân công rõ trách nhiệm cho các bộ phận, cá nhân có liên quan; chủ động bố trí nhân lực có trình độ chuyên môn phù hợp, bảo đảm đáp ứng yêu cầu nhiệm vụ trong tình hình mới.

4. Tăng cường công tác phối hợp, trao đổi, chia sẻ thông tin giữa các cơ quan, đơn vị trong việc phòng ngừa, phát hiện, xử lý các hành vi vi phạm pháp luật về an ninh mạng; chủ động kết nối với các hệ thống giám sát, cảnh báo sớm của tỉnh; kịp thời báo cáo, đề xuất cấp có thẩm quyền xử lý các vấn đề phát sinh.

5. Chủ động bố trí kinh phí trong dự toán ngân sách hằng năm được giao để triển khai thực hiện các nhiệm vụ của Kế hoạch; đồng thời, tăng cường huy động các nguồn lực hợp pháp khác; bảo đảm việc sử dụng kinh phí đúng mục đích, tiết kiệm, hiệu quả, tránh thất thoát, lãng phí.

6. Chế độ thông tin, báo cáo định kỳ

Các sở, ban, ngành, đơn vị cấp tỉnh; UBND các xã, phường và các đơn vị có liên quan có trách nhiệm tổ chức theo dõi, đánh giá tình hình, kết quả triển khai thực hiện các nhiệm vụ được giao tại Kế hoạch này; thực hiện chế độ báo cáo định kỳ 06 tháng (trước ngày 10/6), hằng năm (trước ngày 10/12) và báo cáo đột xuất khi có yêu cầu hoặc khi xảy ra vụ việc, sự cố nghiêm trọng liên quan đến an ninh mạng thuộc phạm vi quản lý.

Công an tỉnh là cơ quan đầu mối có trách nhiệm tổng hợp tình hình, kết quả triển khai thực hiện Kế hoạch trên địa bàn tỉnh; tham mưu cho UBND tỉnh báo cáo các bộ, ngành trung ương theo quy định; đồng thời chủ động đề xuất các giải pháp tháo gỡ khó khăn, vướng mắc phát sinh trong quá trình thực hiện.

7. Sơ kết, tổng kết việc triển khai thực hiện Kế hoạch

Định kỳ hằng năm tổ chức sơ kết, đánh giá kết quả triển khai thực hiện Kế hoạch; kịp thời biểu dương, khen thưởng các tập thể, cá nhân có thành tích xuất sắc; đồng thời chấn chỉnh, khắc phục các tồn tại, hạn chế trong quá trình tổ chức thực hiện.

Căn cứ yêu cầu thực tiễn và hướng dẫn của các bộ, ngành trung ương, tổ chức tổng kết việc thực hiện Kế hoạch theo từng giai đoạn; rà soát, cập nhật, điều chỉnh các mục tiêu, nhiệm vụ, giải pháp bảo đảm phù hợp với tình hình thực tế, yêu cầu phát triển khoa học công nghệ, chuyển đổi số và công tác bảo đảm an ninh mạng trong từng thời kỳ.

8. Công tác kiểm tra, giám sát việc thực hiện Kế hoạch

Công an tỉnh chủ trì, phối hợp với các sở, ban, ngành, đơn vị có liên quan tổ chức kiểm tra, giám sát việc triển khai thực hiện Kế hoạch tại các cơ quan, đơn

vị, địa phương; kịp thời phát hiện, hướng dẫn khắc phục các tồn tại, hạn chế, thiếu sót trong công tác bảo đảm an ninh mạng.

Các cơ quan, đơn vị, địa phương có trách nhiệm tự kiểm tra, đánh giá tình hình triển khai thực hiện các nhiệm vụ được giao; chủ động rà soát, khắc phục các nguy cơ, lỗ hổng, điểm yếu về an ninh mạng thuộc phạm vi quản lý; nghiêm túc thực hiện các yêu cầu, kiến nghị, hướng dẫn của cơ quan có thẩm quyền trong công tác bảo đảm an ninh mạng.

Quá trình thực hiện nếu phát sinh khó khăn, vướng mắc, các cơ quan, đơn vị, địa phương kịp thời trao đổi về Công an tỉnh để tổng hợp báo cáo, tham mưu cho UBND tỉnh xem xét, giải quyết theo quy định./.

Nơi nhận:

- Văn phòng Chính phủ
- Bộ Công an (A05)
- Thường trực: Tỉnh ủy, HĐND tỉnh
- Chủ tịch UBND tỉnh
- Các Phó Chủ tịch UBND tỉnh;
- Ủy ban MTTQ Việt Nam tỉnh;
- Công an tỉnh;
- Các sở, ban, ngành, đơn vị, đoàn thể cấp tỉnh;
- Đảng ủy, UBND các xã, phường;
- Lưu: VT, NN, TDNC.

(để b/c);

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH



Cao Văn Cường