

Số: /KH-UBND

Đồng Tháp, ngày tháng năm 2026

KẾ HOẠCH
Công tác bảo đảm an ninh, an toàn thông tin mạng
trên địa bàn tỉnh Đồng Tháp năm 2026

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; Chỉ thị số 14/CT-TTg ngày 07/6/2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam; Chỉ thị số 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ về đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng Việt Nam; Chỉ thị số 09/CT-TTg ngày 23/02/2024 của Thủ tướng Chính phủ về tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ và Công điện số 33/CĐ-TTg ngày 07/4/2024 của Thủ tướng Chính phủ về tăng cường bảo đảm an toàn thông tin mạng, Ủy ban nhân dân tỉnh (UBND tỉnh) ban hành Kế hoạch công tác bảo đảm an ninh, an toàn thông tin mạng trên địa bàn tỉnh Đồng Tháp năm 2026, với các nội dung như sau:

I. MỤC ĐÍCH - YÊU CẦU

1. Mục đích

- Nhằm thống nhất trong công tác chỉ đạo của các cấp, các ngành tổ chức thực hiện đồng bộ các nhiệm vụ, giải pháp bảo đảm an ninh, an toàn thông tin mạng cho các hệ thống thông tin (HTTT) quan trọng của các cơ quan Đảng, Nhà nước và các tổ chức chính trị - xã hội trên địa bàn tỉnh, nhất là các HTTT phục vụ chính quyền điện tử, chính quyền số, góp phần tạo niềm tin cho người dân, doanh nghiệp, bảo đảm quốc phòng - an ninh trên địa bàn tỉnh.

- Lấy phòng ngừa chủ động là chính, đi trước một bước, không để bị động, bất ngờ trong mọi tình huống. Mọi nguy cơ, thách thức về an ninh, an toàn thông tin mạng phải được nhận diện và xử lý từ sớm.

- Nâng cao nhận thức, kỹ năng về an toàn thông tin mạng cho cán bộ, công chức, viên chức và người dân, nhất là người đứng đầu các cơ quan, đơn vị, cán bộ trực tiếp quản trị, vận hành HTTT.

2. Yêu cầu

- Các cơ quan, đơn vị nhận thức đầy đủ, sâu sắc về vai trò, tầm quan trọng của công tác bảo đảm an ninh, an toàn thông tin mạng trong phát triển kinh tế - xã hội, bảo đảm quốc phòng - an ninh tại địa phương. Người đứng đầu trực tiếp phụ trách, chỉ đạo và chịu trách nhiệm về kết quả thực hiện.

- Tuân thủ các quy định của pháp luật về an toàn thông tin mạng, đặc biệt là bảo đảm an toàn HTTT theo cấp độ.

- Các giải pháp, nhiệm vụ phải được triển khai đồng bộ, thống nhất từ cấp tỉnh đến cấp cơ sở và các cơ quan, đơn vị liên quan. Huy động sức mạnh của cả hệ thống chính trị, doanh nghiệp và người dân vào công tác bảo đảm an ninh, an toàn thông tin mạng trên địa bàn tỉnh.

- Kinh phí đầu tư cho an ninh mạng, an toàn thông tin đảm bảo tỷ lệ tối thiểu 15% tổng kinh phí triển khai đề án, dự án ứng dụng công nghệ thông tin.

II. NHIỆM VỤ, GIẢI PHÁP TRỌNG TÂM

1. Tăng cường lãnh đạo, chỉ đạo, điều hành công tác bảo đảm an ninh, an toàn thông tin mạng

- Tiếp tục triển khai Chương trình hành động số 10-CTr/TU, ngày 13/8/2025 của Ban Thường vụ Tỉnh ủy Đồng Tháp về 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 Đồng Tháp; Thông báo Kết luận số 06-TB/CQTTBCĐ, ngày 27/9/2025 của Cơ quan Thường trực Ban Chỉ đạo Trung ương về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số; triển khai các nhiệm vụ bảo đảm an ninh, an toàn thông tin mạng theo chủ trương của Chính phủ, Bộ Công an, các kết luận chỉ đạo định kỳ, đột xuất của Tỉnh ủy, UBND tỉnh,... nhằm phục vụ mục tiêu phát triển Chính quyền số, kinh tế số, xã hội số, tăng năng suất lao động, tạo động lực tăng trưởng xanh, bảo đảm phát triển bền vững.

- Thống nhất nhận thức về tầm quan trọng của công tác bảo đảm an ninh, an toàn thông tin mạng, xem đây là nhiệm vụ trọng yếu, thường xuyên, xuyên suốt, liên tục, vừa cấp bách trước mắt, vừa chiến lược lâu dài, gắn liền với sự phát triển kinh tế - xã hội.

- Người đứng đầu các cơ quan, tổ chức từ tỉnh đến cơ sở chịu trách nhiệm lãnh đạo, chỉ đạo, kiểm tra, đôn đốc công tác bảo đảm an ninh, an toàn thông tin mạng. Phát huy sức mạnh tổng hợp của cả hệ thống chính trị và toàn dân, trong đó Nhà nước giữ vai trò chủ đạo, lực lượng chuyên trách bảo đảm an ninh, an toàn thông tin mạng là nòng cốt.

2. Nâng cao năng lực quản lý và hoàn thiện pháp lý

- Hoàn thành việc lập hồ sơ và thẩm định phê duyệt hồ sơ đề xuất cấp độ an toàn HTTT cho 100% các HTTT trên địa bàn tỉnh theo quy định pháp luật.

- Thường xuyên rà soát, xây dựng mới hoặc điều chỉnh, bổ sung quy chế, quy trình nội bộ về vận hành, khai thác và ứng cứu sự cố cho HTTT; quy trình sao lưu và phục hồi dữ liệu đảm bảo đúng theo quy định.

- Cơ quan chủ quản, đơn vị vận hành các cơ sở dữ liệu, HTTT từ tỉnh đến cơ sở định kỳ tổ chức đánh giá tổng thể về an ninh mạng, bảo mật thông tin, an toàn dữ liệu đối với HTTT và nguồn nhân lực thuộc phạm vi quản lý.

- Tổ chức kiểm tra, đánh giá định kỳ hoặc đột xuất việc tuân thủ quy định của pháp luật về an toàn thông tin mạng đối với các đơn vị, tổ chức, doanh nghiệp đang vận hành HTTT trên địa bàn tỉnh.

3. Tăng cường các giải pháp, hoàn thiện về hạ tầng, kỹ thuật

- Triển khai đầy đủ các biện pháp, phương án bảo đảm an toàn thông tin theo yêu cầu của cấp độ đã được phê duyệt cho từng HTTT.

- Xây dựng và củng cố năng lực tự chủ, tự cường về công nghệ, con người và cơ chế quản trị là nền tảng cốt lõi để bảo vệ an toàn HTTT. Phải ưu tiên nguồn lực để làm chủ các công nghệ lõi, phát triển, sử dụng sản phẩm công nghiệp an ninh mạng “Make in Vietnam” bền vững.

- Đầu tư, duy trì và vận hành hiệu quả Hệ thống giám sát an ninh mạng tỉnh (SOC), bảo đảm các HTTT cấp độ 3 trở lên được giám sát, bảo vệ đầy đủ các lớp (*lớp mạng, lớp ứng dụng, lớp cơ sở dữ liệu, lớp thiết bị đầu cuối*); tiếp tục đầu tư và vận hành tốt Hệ thống giám sát mã độc tập trung. Duy trì kết nối với Trung tâm An ninh mạng quốc gia để được hỗ trợ giám sát, phân tích, cảnh báo sớm các nguy cơ về an toàn thông tin mạng và tấn công mạng.

- Thường xuyên tiến hành rà quét lỗ hổng bảo mật trên Cổng, Trang thông tin điện tử của các cơ quan Đảng, Nhà nước trên địa bàn tỉnh nhằm phát hiện, xử lý, khắc phục kịp thời các lỗ hổng bảo mật, nguy cơ mất an toàn HTTT, giảm thiểu thiệt hại, rủi ro.

4. Nâng cao khả năng ứng cứu sự cố và tổ chức diễn tập thực chiến

- Thường xuyên rà soát, kiện toàn Đội Ứng cứu sự cố an toàn thông tin mạng của tỉnh, đảm bảo nhân lực và năng lực để xử lý khi có sự cố an toàn thông tin mạng xảy ra.

- Tổ chức diễn tập thực chiến ứng cứu sự cố an toàn thông tin mạng cho hệ thống thông tin dùng chung của tỉnh (ít nhất 01 lần), nhằm đánh giá năng lực của cán bộ chuyên trách của các cơ quan, đơn vị, nhất là thành viên của Đội Ứng cứu sự cố tỉnh, cũng như đánh giá các quy trình, phương án ứng cứu sự cố, đồng thời trang bị thêm kỹ năng xử lý khi có sự cố xảy ra.

- Đội Ứng cứu sự cố an toàn thông tin mạng của tỉnh tăng cường mở rộng mạng lưới liên kết các chuyên gia an ninh mạng trong và ngoài tỉnh tham gia hỗ trợ công tác bảo đảm an ninh mạng; kết nối, chia sẻ thông tin về các cuộc tấn công, lỗ hổng bảo mật với Trung tâm An ninh mạng quốc gia; tham gia luyện tập, diễn tập an toàn thông tin, an ninh mạng quốc gia.

5. Nâng cao nhận thức và đào tạo phát triển nguồn nhân lực an ninh, an toàn thông tin mạng

- Nâng cao nhận thức của cán bộ, đảng viên và nhân dân về tầm quan trọng của công tác bảo đảm an ninh, an toàn thông tin mạng. Tuyên truyền, phổ biến pháp luật về an ninh mạng, kiến thức, kỹ năng cơ bản về an toàn thông tin mạng cho cán bộ, công chức và người dân có chiều sâu, đa dạng về nội dung và hình thức. Đưa các nội dung kiến thức, kỹ năng cơ bản về an ninh, an toàn thông tin mạng vào chương trình giáo dục phổ thông, giáo dục nghề và đại học giúp thế hệ trẻ có ý thức từ sớm. Tăng cường tuyên truyền, phổ biến, đào tạo kiến thức an ninh mạng trên nền tảng “Bình dân học vụ số”, nhất là các quy định và kỹ năng bảo vệ dữ liệu cá nhân, phòng chống tội phạm lừa đảo trên không gian mạng,... Người đứng đầu các cơ quan, đơn vị phải nêu cao trách nhiệm trong việc chỉ đạo, tổ chức thực hiện công tác an toàn thông tin mạng.

- Các sở ban, ngành, địa phương thường xuyên rà soát, đánh giá, xác định nhu cầu nhân lực bảo đảm an ninh, an toàn thông tin mạng và có kế hoạch bổ sung đào tạo, bồi dưỡng, bảo đảm đáp ứng yêu cầu trong tình hình mới.

- Tổ chức các khóa đào tạo thực tế, tập huấn chuyên sâu về an toàn thông tin mạng cho đội ngũ cán bộ chuyên trách an ninh mạng, công nghệ thông tin của các cơ quan, đơn vị, địa phương.

III. KINH PHÍ THỰC HIỆN

Kinh phí thực hiện Kế hoạch này được đảm bảo từ nguồn ngân sách Nhà nước theo phân cấp ngân sách hiện hành và nguồn tài chính hợp pháp khác (nếu có).

IV. TỔ CHỨC THỰC HIỆN

1. Công an tỉnh

- Là cơ quan đầu mối tham mưu cho UBND tỉnh tổ chức triển khai Kế hoạch này. Kiểm tra, hướng dẫn, đôn đốc các cơ quan, đơn vị thực hiện có hiệu quả Kế hoạch này và tổng hợp, báo cáo định kỳ (*trước 15/12*) hoặc đột xuất cho UBND tỉnh và Bộ Công an về tình hình, công tác bảo đảm an ninh, an toàn thông tin mạng trên địa bàn tỉnh.

- Thực hiện thẩm định, phê duyệt cấp độ an toàn thông tin mạng đối với hồ sơ đề xuất cấp độ theo quy định.

- Chủ trì, phối hợp với các cơ quan, đơn vị có liên quan tổ chức thực thi, đôn đốc, kiểm tra, giám sát định kỳ hoặc đột xuất công tác bảo đảm an ninh, an toàn thông tin mạng; kịp thời phát hiện và xử lý theo thẩm quyền đối với các hành vi vi phạm an toàn thông tin mạng trên địa bàn tỉnh.

- Tham mưu tổ chức đào tạo, bồi dưỡng chuyên sâu về an toàn thông tin mạng cho lực lượng chuyên trách, cán bộ, công chức, viên chức, người lao động thực hiện công tác bảo đảm an toàn thông tin mạng của các cơ quan, đơn vị.

- Chủ trì, phối hợp Sở Khoa học và Công nghệ, Đội Ứng cứu sự cố an toàn thông tin mạng tỉnh tổ chức diễn tập bảo đảm an toàn thông tin mạng đối với các HTTT dùng chung do UBND tỉnh triển khai.

- Tham mưu UBND tỉnh triển khai, quản lý, vận hành các hệ thống hạ tầng kỹ thuật bảo đảm an ninh, an toàn thông tin mạng tập trung (hệ thống phòng, chống mã độc; hệ thống giám sát an toàn thông tin mạng) để kịp thời phát hiện, xử lý các vấn đề liên quan đến an toàn thông tin mạng, giảm thiểu tấn công mạng; hỗ trợ giám sát an toàn thông tin cho các HTTT của các cơ quan, đơn vị.

- Chủ trì tổ chức rà quét lỗ hổng bảo mật các HTTT trên địa bàn tỉnh, phát hiện cảnh báo, xử lý từ sớm không để xảy ra sự cố nghiêm trọng.

- Tổng hợp nhu cầu kinh phí thực hiện công tác bảo đảm an ninh, an toàn thông tin năm 2026 của các đơn vị, địa phương, phối hợp Sở Tài chính tham mưu cơ quan có thẩm quyền xem xét, bố trí kinh phí.

2. Sở Khoa học và Công nghệ

- Tham mưu UBND tỉnh ban hành các quy định về quản lý, vận hành và bảo đảm an toàn thông tin mạng đối với các HTTT dùng chung do UBND tỉnh

triển khai. Thực hiện xây dựng hồ sơ, đề xuất phê duyệt cấp độ an toàn đối với các HTTT này và triển khai đầy đủ các biện pháp bảo đảm an toàn thông tin theo hồ sơ đã được phê duyệt. Định kỳ đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin đã triển khai, báo cáo đề xuất UBND tỉnh điều chỉnh nếu cần thiết.

- Phối hợp Công an tỉnh, Đội Ứng cứu sự cố an toàn thông tin mạng tỉnh tổ chức diễn tập bảo đảm an toàn thông tin mạng đối với các HTTT dùng chung do UBND tỉnh triển khai.

- Phối hợp Công an tỉnh trong công tác thanh tra, kiểm tra về an toàn thông tin mạng.

- Tổ chức hoạt động kết nối, hợp tác với các tập đoàn, doanh nghiệp viễn thông, công nghệ số lớn trong và ngoài nước để hỗ trợ nghiên cứu, triển khai, cung cấp các nền tảng, giải pháp, dịch vụ công nghệ số phù hợp cho sở, ban, ngành, địa phương.

3. Sở Tài chính

Trên cơ sở kinh phí thực hiện Kế hoạch này của các đơn vị, địa phương có liên quan lập do Công an tỉnh tổng hợp, Sở Tài chính cân đối nguồn kinh phí tham mưu cơ quan có thẩm quyền xem xét, bố trí kinh phí cho các đơn vị, địa phương có liên quan tổ chức thực hiện theo quy định.

4. Sở Giáo dục và Đào tạo

Nghiên cứu tích hợp các nội dung đào tạo kiến thức, kỹ năng cơ bản về an ninh, an toàn thông tin mạng vào chương trình giáo dục phổ thông và các hoạt động ngoại khóa phù hợp với từng cấp học trên địa bàn tỉnh. Chỉ đạo các cơ sở giáo dục phổ thông tăng cường tuyên truyền, nâng cao nhận thức cho học sinh về kỹ năng bảo vệ dữ liệu cá nhân và phòng chống lừa đảo trên không gian mạng. Phối hợp với các cơ quan, đơn vị trên địa bàn trong việc tổ chức các cuộc thi, sự kiện học thuật, nghiên cứu sáng tạo về an toàn thông tin nhằm định hướng nghề nghiệp cho học sinh phổ thông.

5. Sở Nội vụ

Phối hợp các sở, ngành, địa phương thực hiện chính sách thu hút, trọng dụng người có tài năng trong lĩnh vực an ninh mạng, an toàn thông tin làm việc trong cơ quan, tổ chức, đơn vị của Đảng Cộng sản Việt Nam, Nhà nước, Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội theo phân cấp quản lý.

6. Các sở, ban, ngành tỉnh; UBND các xã, phường

- Căn cứ nhu cầu kinh phí thực hiện công tác bảo đảm an ninh, an toàn thông tin năm 2026, lập dự toán kinh phí (*đảm bảo đạt tỷ lệ tối thiểu 15% tổng kinh phí triển khai đề án, dự án ứng dụng công nghệ thông tin*) gửi về Công an tỉnh (*qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao*) trước ngày **10/02/2026** để tổng hợp báo cáo cấp có thẩm quyền phê duyệt.

- Căn cứ chức năng, nhiệm vụ của đơn vị mình chủ động phối hợp với các sở, ngành và đơn vị liên quan triển khai thực hiện có hiệu quả Kế hoạch này; định kỳ năm (***trước ngày 10/12***) hoặc đột xuất khi có yêu cầu báo cáo kết quả thực hiện các nhiệm vụ gửi Công an tỉnh (*qua Phòng An ninh mạng và phòng, chống*

tội phạm sử dụng công nghệ cao) để tổng hợp báo cáo UBND tỉnh, Bộ Công an theo quy định.

7. Các Trường Đại học, Cao đẳng, các cơ sở giáo dục nghề nghiệp trên địa bàn tỉnh

- Tăng cường tuyên truyền, tổ chức các hoạt động ngoại khóa cho sinh viên nhằm nâng cao nhận thức, kỹ năng bảo vệ dữ liệu cá nhân, phòng chống lừa đảo trên không gian mạng.

- Nghiên cứu, tham mưu mở chuyên ngành đào tạo liên quan bảo đảm an ninh, an toàn thông tin để tạo nguồn nhân lực an ninh mạng chất lượng cao cho địa phương.

8. Đề nghị các doanh nghiệp viễn thông, công nghệ thông tin

Chủ động thực hiện công tác bảo đảm an toàn thông tin mạng trong hoạt động của doanh nghiệp, phát triển hạ tầng số, nền tảng số, làm chủ công nghệ. Tham gia tư vấn các giải pháp tạo nền móng và cung cấp các nền tảng, ứng dụng, dịch vụ, giải pháp an toàn thông tin mạng phù hợp cho cơ quan, tổ chức, doanh nghiệp, người dân trên địa bàn tỉnh để thực hiện phát triển chính quyền số, kinh tế số, công dân số, xã hội số theo mục tiêu đã đề ra trong Kế hoạch này.

Trong quá trình triển khai thực hiện Kế hoạch nếu có khó khăn, vướng mắc, các cơ quan, đơn vị và địa phương kịp thời phản ánh về Công an tỉnh để phối hợp giải quyết; trường hợp vượt quá thẩm quyền, Công an tỉnh tổng hợp, trình UBND tỉnh xem xét, quyết định./.

(Kèm theo Phụ lục - Phân công theo dõi, thực hiện các nhiệm vụ, chỉ tiêu Kế hoạch năm 2026)

Nơi nhận:

- Bộ Công an (Cục A05);
- TTTU, TT HĐND tỉnh;
- Các PCT UBND tỉnh;
- Lãnh đạo VP UBND tỉnh;
- Các sở, ban, ngành tỉnh;
- Các Trường Đại học, Cao đẳng, các cơ sở giáo dục nghề nghiệp trên địa bàn tỉnh;
- Các doanh nghiệp viễn thông, công nghệ thông tin trên địa bàn tỉnh;
- UBND các xã, phường;
- Lưu: VT, TCDNC(Ngọc).

**TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH**

Phạm Thành Ngại