BAN CHẤP HÀNH TRUNG ƯƠNG
BAN CHỈ ĐẠO TRUNG ƯƠNG
VỀ PHÁT TRIỂN KHOA HỌC, CÔNG NGHỆ, ĐỔI MỚI SÁNG TẠO VÀ CHUYỂN ĐỔI SỐ
*
Số 04-KH/BCĐTW

ĐẢNG CỘNG SẢN VIỆT NAM

Hà Nội, ngày 05 tháng 01 năm 2026

KẾ HOẠCH
Bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong hệ thống chính trị

I- CĂN CỨ LẬP KẾ HOẠCH

- 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;

- Quyết định số 229-QĐ/TW, ngày 10/01/2025 của Bộ Chính trị về thành lập Ban Chỉ đạo Trung ương về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số;

- Quy định số 230-QĐ/TW, ngày 10/01/2025 của Bộ Chính trị về chức năng, nhiệm vụ, quyền hạn, chế độ làm việc, quan hệ công tác của Ban Chỉ đạo Trung ương về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số;

- Quy chế làm việc số 01-QC/BCĐTW, ngày 28/02/2025 của Ban Chỉ đạo Trung ương về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số;

- 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,

Ban Chỉ đạo Trung ương về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số *(sau đây gọi tắt là Ban Chỉ đạo Trung ương)* ban hành Kế hoạch bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong hệ thống chính trị, cụ thể như sau:

II- MỤC TIÊU VÀ YÊU CẦU

1. Mục tiêu chung

Xây dựng không gian mạng quốc gia an toàn, vững mạnh, có năng lực phòng vệ tốt và khả năng chống chịu cao, bảo vệ vững chắc chủ quyền, an ninh và lợi ích của quốc gia trên không gian mạng.

2. Mục tiêu cụ thể

a) Trong năm 2026

- Về công tác lãnh đạo, chỉ đạo: Tạo chuyển biến mạnh mẽ, về nhận thức và hành động trong toàn hệ thống chính trị và xã hội.

- Về thể chế: Hoàn thiện cơ chế pháp lý để khuyến khích đổi mới sáng tạo, tạo điều kiện cho doanh nghiệp mới tham gia thị trường, tiếp tục được hoàn thiện gỡ bỏ các rào cản thủ tục.

- Về hạ tầng: Xây dựng và phát triển hạ tầng an ninh mạng quốc gia hiện đại, đồng bộ, đủ năng lực bảo vệ chủ quyền không gian mạng: (1) Các hệ thống thông tin của cơ quan Đảng, Nhà nước, Mặt trận Tổ quốc và các tổ chức chính trị - xã hội được rà soát, khắc phục các lỗ hổng, điểm yếu an ninh mạng. (2) Các hệ thống thông tin quan trọng thuộc danh mục được ưu tiên bảo vệ của hệ thống chính trị từ cấp độ 3 trở lên *(trừ hệ thống thông tin trong lĩnh vực quân sự, quốc phòng và cơ yếu)* được kết nối, chia sẻ thông tin, dữ liệu giám sát an ninh mạng 24/7 với Trung tâm An ninh mạng quốc gia (Bộ Công an). (3) Xây dựng và ban hành các tiêu chuẩn, quy chuẩn kỹ thuật cho sản phẩm, dịch vụ an ninh mạng. (4) Bảo đảm hạ tầng mật mã quốc gia hoạt động ổn định, bảo mật phục vụ trao đổi dữ liệu bí mật nhà nước từ trung ương đến 100% cấp xã, phường và đặc khu.

- Nhân lực: Nâng cao nhận thức của cán bộ, đảng viên và người dân về bảo mật thông tin, an ninh mạng và an ninh dữ liệu; Đào tạo, bồi dưỡng đội ngũ chuyên gia an ninh mạng chất lượng cao.

- Quản trị: Tăng cường kỷ luật, kỷ cương trong quản lý nhà nước về an ninh mạng; thực hiện quản trị an ninh mạng dựa trên đánh giá rủi ro, tuân thủ tiêu chuẩn, quy chuẩn kỹ thuật.

- Công nghệ: Thúc đẩy ứng dụng các công nghệ tiên tiến như trí tuệ nhân tạo, phân tích dữ liệu lớn, giám sát thông minh để phát hiện sớm và xử lý kịp thời các mối đe doạ mạng. Chuyển đổi sang mô hình phòng thủ chủ động, các giải pháp mã hoá hiện đại phục vụ bảo vệ dữ liệu quan trọng, dữ liệu bí mật và giao dịch của Nhà nước. Khuyến khích nghiên cứu, phát triển và làm chủ các công nghệ an ninh mạng thế hệ mới, tăng cường năng lực tự chủ công nghệ, hình thành hệ sinh thái công nghiệp an ninh mạng quốc gia vững mạnh.

b) Đến năm 2030

- Vị thế quốc gia: Việt Nam tiếp tục được xếp hạng trong nhóm 20 quốc gia có mức đánh giá cao về Chỉ số An toàn, an ninh mạng toàn cầu (GCI) của Liên minh Viễn thông Quốc tế (ITU).

- Thể chế: Hoàn thiện cơ chế pháp lý để khuyến khích đổi mới sáng tạo, tạo điều kiện cho doanh nghiệp mới tham gia thị trường, sản phẩm, giải pháp an ninh mạng chất lượng có cơ hội phát triển. Các quy định của pháp luật đủ sức răn đe, và phản ứng nhanh với các hành vi vi phạm pháp luật trên không gian mạng.

- Hạ tầng: Xây dựng và đưa vào vận hành hiệu quả kiến trúc bảo vệ an ninh mạng quốc gia đa lớp hiện đại, đồng bộ, hiệu quả bảo đảm chủ quyền quốc gia trên không gian mạng, bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu; ban hành quy hoạch hạ tầng công nghệ thông tin tổng thể từ Trung ương đến địa phương.

- Nhân lực: Đào tạo và xây dựng được đội ngũ 10.000 chuyên gia an ninh mạng trình độ cao, đáp ứng nhu cầu trong nước và quốc tế.

- Quản trị: Các bộ, ngành, địa phương và các tổ chức vận hành hạ tầng thông tin quan trọng triển khai và áp dụng hiệu quả Khung quản trị rủi ro an ninh mạng quốc gia.

- Công nghệ: Tỉ trọng sản phẩm, dịch vụ an ninh mạng "Make in Vietnam" chiếm trên 50% thị trường trong nước và bắt đầu hình thành năng lực xuất khẩu đạt chuẩn quốc tế. Tự chủ nghiên cứu, sản xuất và làm chủ công nghệ lõi đối với các sản phẩm an ninh mạng, bảo mật thông tin và an ninh dữ liệu.

c) Tầm nhìn chiến lược đến năm 2045

Xây dựng nền an ninh mạng quốc gia bền vững, tự chủ, có năng lực cạnh tranh toàn cầu. Hình thành đội ngũ chuyên gia đầu ngành, nhà khoa học công nghệ số trình độ quốc tế; làm chủ các công nghệ cốt lõi, giảm phụ thuộc nhập khẩu. Phát triển hạ tầng an ninh mạng và hạ tầng số hiện đại; xây dựng các trung tâm đổi mới sáng tạo, khu công nghiệp công nghệ cao; doanh nghiệp trong nước trở thành trụ cột của ngành công nghiệp an ninh mạng Việt Nam.

3. Yêu cầu

- Kế hoạch phải được quán triệt và triển khai thống nhất trong toàn bộ hệ thống chính trị, tránh dàn trải, cục bộ, thiếu tập trung.

- Nhiệm vụ phải được tổ chức thực hiện với quyết tâm cao, có sản phẩm cụ thể, đo lường được, bảo đảm tiến độ và hiệu quả thực chất.

- Phát huy tối đa tiềm năng, trí tuệ Việt Nam, gắn với tiếp thu, làm chủ và ứng dụng hiệu quả các thành tựu công nghệ, kỹ thuật tiên tiến của thế giới.

- Gắn trách nhiệm người đứng đầu với kết quả bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu; coi đây là tiêu chí quan trọng trong đánh giá, quy hoạch, bổ nhiệm cán bộ lãnh đạo, quản lý các cấp.

III- NHIỆM VỤ TRỌNG TÂM NĂM 2026

1. Kiện toàn Ban Chỉ đạo An toàn, an ninh mạng Quốc gia và các tiểu ban tại các Bộ, ngành, địa phương.

2. Các cơ quan chủ quản các cơ sở dữ liệu, hệ thống thông tin trong hệ thống chính trị từ Trung ương đến cơ sở có trách nhiệm: (i) Rà soát, khắc phục tổng thể về an ninh mạng, bảo mật thông tin, an ninh dữ liệu đối với hệ thống thông tin theo tiêu chuẩn TCVN 14423: 2025 và nguồn nhân lực thuộc phạm vi quản lý. (ii) Triển khai giám sát an ninh mạng tại cơ quan, đơn vị thuộc phạm vi quản lý. (iii) Báo cáo định kỳ và đột xuất kết quả, tiến độ và mức độ tuân thủ về cơ quan có thẩm quyền; kiến nghị biện pháp hoàn thiện thể chế, tiêu chuẩn và phân bổ nguồn lực khi cần. (iv) Xác định trách nhiệm của người đứng đầu về an ninh mạng.

3. Nâng cao năng lực của Trung tâm An ninh mạng quốc gia; mở rộng kết nối, chia sẻ dữ liệu giám sát, cảnh báo an ninh mạng với các hệ thống thông tin quan trọng của hệ thống chính trị từ cấp độ 3 trở lên (trừ các hệ thống thông tin trong lĩnh vực quân sự, quốc phòng và cơ yếu); thiết lập kênh kết nối trao đổi thông tin, dữ liệu phục vụ giám sát, điều phối ứng cứu, khắc phục sự cố an toàn thông tin, an ninh mạng.

4. Xây dựng, vận hành Hệ thống phòng vệ mạng quốc gia nhằm bảo vệ an ninh mạng vòng ngoài cho các hệ thống thông tin, tài nguyên trọng yếu trên Internet của các cơ quan ban, bộ, ngành, địa phương, cơ quan, doanh nghiệp Việt Nam.

5. Ban hành các quy định, tài liệu hướng dẫn về kiểm tra, đánh giá, bảo đảm an ninh mạng, an toàn thông tin cho các cơ sở dữ liệu, hệ thống dùng chung trong hệ thống chính trị; định kỳ tổ chức kiểm tra, đánh giá việc thực hiện các quy định đảm bảo an ninh mạng, an toàn thông tin theo quy định.

6. Ban hành cơ chế ưu đãi đặc biệt và chính sách ưu tiên sử dụng sản phẩm, giải pháp, dịch vụ an ninh mạng, bảo mật thông tin và an ninh dữ liệu "Make in Vietnam"; từng bước hình thành hệ sinh thái an ninh mạng quốc gia vững mạnh, nâng cao năng lực cạnh tranh đáp ứng nhu cầu xuất khẩu, tham gia sâu vào chuỗi giá trị toàn cầu.

7. Rà soát, trình cấp có thẩm quyền xem xét ban hành hoặc điều chỉnh quy hoạch hạ tầng công nghệ thông tin tổng thể từ Trung ương đến địa phương theo hướng tập trung, chuẩn hoá trung tâm dữ liệu. Đầu tư, nâng cấp hạ tầng công nghệ thông tin đáp ứng yêu cầu và tuân thủ quy hoạch đã được ban hành.

IV- NHIỆM VỤ ĐẾN NĂM 2030

1. Nâng cao nhận thức cho toàn hệ thống chính trị và người dân

a) Triển khai các chương trình đào tạo, bồi dưỡng, phổ biến kiến thức an ninh mạng trên nền tảng "Bình dân học vụ số".

b) Đẩy mạnh truyền thông đại chúng và trên mạng xã hội cho người dân kỹ năng nhận diện, phòng, chống lừa đảo, tiếp nhận và xử lý phản ánh sự cố.

c) Đưa các nội dung kiến thức, kỹ năng cơ bản về an ninh mạng vào chương trình giáo dục phổ thông (từ Trung học cơ sở đến Trung học phổ thông), giáo dục nghề nghiệp và đại học.

d) Triển khai các giải pháp định danh và đánh giá tín nhiệm mạng đối với các tổ chức, cá nhân có ảnh hưởng trên không gian mạng; củng cố lòng tin, trách nhiệm của người dân khi hoạt động, tương tác, làm việc trên không gian mạng.

đ) Đưa tiêu chí bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu vào đánh giá xếp loại thi đua, khen thưởng của cơ quan, tổ chức, đơn vị.

2. Xây dựng và hoàn thiện thể chế, khung pháp lý

a) Tiếp tục rà soát, sửa đổi, bổ sung, hoàn thiện hành lang pháp lý cho an ninh mạng, bảo mật thông tin, an ninh dữ liệu, bảo đảm thể chế đi trước một bước.

b) Hoàn thiện các tiêu chuẩn quốc gia và quy chuẩn kỹ thuật đối với các sản phẩm, dịch vụ an ninh mạng, bảo mật thông tin, áp dụng trước hết đối với hạ tầng thông tin quan trọng quốc gia, hệ thống thông tin của các cơ quan trong hệ thống chính trị mà có ảnh hưởng trực tiếp đến an ninh quốc gia, trật tự xã hội và đời sống nhân dân.

c) Xây dựng Khung quản trị rủi ro an ninh mạng quốc gia và chỉ số đánh giá năng lực bảo đảm an ninh mạng.

d) Hoàn thiện các cơ chế trao đổi, chia sẻ thông tin trong nước và quốc tế về an ninh mạng.

3. Phát triển hạ tầng an ninh mạng hiện đại, đồng bộ, đáp ứng yêu cầu bảo vệ chủ quyền quốc gia trên không gian mạng

a) Triển khai kiến trúc bảo vệ an ninh mạng quốc gia đa lớp hỗ trợ bảo vệ cho toàn bộ hạ tầng mạng Internet Việt Nam và các hệ thống thông tin của bộ, ngành, địa phương, tổ chức, doanh nghiệp.

b) Quy hoạch và triển khai đồng bộ các nhóm giải pháp: (i) Bảo vệ hạ tầng mạng. (ii) Bảo vệ thiết bị đầu cuối. (iii) Bảo vệ ứng dụng, dịch vụ. (iv) Bảo vệ dữ liệu. (v) Bảo vệ người dùng.

c) Tập trung nguồn lực quốc gia để nghiên cứu, làm chủ các công nghệ lõi chiến lược như công nghệ mật mã, thiết kế và sản xuất chip bảo mật "Make in Vietnam"; nghiên cứu, phát triển mã hoá kháng lượng tử để bảo vệ bí mật nhà nước; khuyến khích xã hội hoá nghiên cứu, phát triển và ứng dụng mật mã dân sự phục vụ bảo mật thông tin.

d) Bảo vệ tuyệt đối an toàn các hệ thống thông tin quan trọng, các cơ sở dữ liệu quốc gia về dân cư, đất đai, tài chính, y tế, giáo dục, bảo hiểm, tư pháp… Thiết lập cơ chế thống nhất về tiêu chuẩn, quy chuẩn bảo mật; bảo đảm an ninh mạng "*ngay từ thiết kế*" đối với các trung tâm dữ liệu quan trọng, các hệ thống số, nền tảng số và ứng dụng mới; khắc phục ngay những lỗ hổng bảo mật trong các hệ thống thông tin. Kết nối, chia sẻ dữ liệu liên thông giữa các ban, bộ, ngành, địa phương trên nguyên tắc bảo mật, an toàn, đúng pháp luật, khắc phục tình trạng cát cứ, phân mảnh dữ liệu.

4. Phát triển công nghiệp an ninh mạng tự chủ và thị trường an ninh mạng cạnh tranh, minh bạch

a) Nghiên cứu xây dựng cơ chế đầu tư cho phát triển hệ sinh thái an ninh mạng, đặc biệt là hệ sinh thái "*Make in Vietnam*"; ưu tiên làm chủ và sản xuất nội địa các sản phẩm an ninh mạng cốt lõi, nền tảng.

b) Xây dựng thị trường cạnh tranh lành mạnh, minh bạch. Hình thành các trung tâm nghiên cứu, vườn ươm hỗ trợ khởi nghiệp và không gian đổi mới sáng tạo để hỗ trợ doanh nghiệp, nhất là các doanh nghiệp khởi nghiệp sáng tạo, thúc đẩy gắn kết giữa nghiên cứu - triển khai - thương mại hoá sản phẩm.

c) Ưu tiên sử dụng các sản phẩm, giải pháp nội địa đáp ứng được các tiêu chuẩn, quy chuẩn trong các dự án, hệ thống trọng yếu nhằm vừa tạo thị trường, vừa thúc đẩy và hỗ trợ doanh nghiệp Việt Nam phát triển. Phù hợp chủ trương nâng cao khả năng tự chủ chiến lược của đất nước.

d) Xây dựng các tiêu chuẩn, quy chuẩn kỹ thuật về mã dân sự để bảo vệ an ninh mạng.

5. Bảo đảm nguồn lực tài chính, ngân sách

Quy định an ninh mạng, bảo mật thông tin, an ninh dữ liệu là thành phần bắt buộc trong mọi dự án công nghệ thông tin; bảo đảm tỉ lệ kinh phí bình quân chi cho các sản phẩm, dịch vụ an ninh mạng, bảo mật thông tin, an ninh dữ liệu đạt tối thiểu 15% trong tổng kinh phí triển khai đề án, dự án, chương trình, kế hoạch đầu tư, ứng dụng, phát triển công nghệ thông tin, bảo đảm hiệu quả, đúng quy định, tránh lãng phí. Nghiên cứu sửa đổi bổ sung các quy định pháp luật có liên quan để tạo cơ chế thông thoáng trong đầu tư, triển khai an ninh mạng, bảo mật thông tin, an ninh dữ liệu.

6. Bảo đảm nguồn nhân lực

a) Xây dựng chương trình đào tạo chuyên sâu, huấn luyện thực tế về công tác an ninh mạng. Tiếp tục hoàn thiện cơ chế, chính sách thu hút, đãi ngộ chuyên gia tham gia phục vụ công tác an ninh mạng quốc gia.

b) Triển khai các chương trình đào tạo, bồi dưỡng, nâng cao năng lực chuyên môn, kỹ năng giám sát, điều tra, ứng phó sự cố, bảo vệ dữ liệu, an ninh mạng, an toàn thông tin, bảo mật và tác chiến bảo vệ chủ quyền quốc gia trên không gian mạng; nâng cao năng lực nghiên cứu, phát triển, làm chủ công nghệ lõi trong an ninh mạng.

c) Tăng cường liên kết giữa Nhà nước - Nhà trường - Doanh nghiệp trong đào tạo, huấn luyện thực chiến. Xây dựng Mạng lưới liên kết các chuyên gia an ninh mạng trong nước và nước ngoài tham gia hỗ trợ công tác bảo đảm an ninh mạng. Mở rộng Liên minh ứng phó, khắc phục sự cố an ninh mạng quốc gia.

d) Tăng cường nhân lực bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu cho ban, bộ, ngành, địa phương theo quy định.

7. Hợp tác quốc tế trên lĩnh vực an ninh mạng

a) Chủ động tham gia xây dựng các khuôn khổ pháp lý, chuẩn mực chung của quốc tế.

b) Sớm đưa Công ước Hà Nội về chống tội phạm mạng 2025 có hiệu lực và thúc đẩy việc thực hiện hiệu quả, thực chất Công ước.

c) Tăng cường hợp tác chia sẻ thông tin, điều tra tội phạm mạng xuyên quốc gia; tham gia diễn tập quốc tế và nghiên cứu thành lập trung tâm đào tạo khu vực tại Việt Nam.

V- TỔ CHỨC THỰC HIỆN

1. Phân công trách nhiệm

a) Ban Chỉ đạo Trung ương

Chịu trách nhiệm chỉ đạo toàn diện việc triển khai Kế hoạch; trực tiếp cho ý kiến chỉ đạo về các chủ trương, cơ chế, chính sách lớn; chỉ đạo tháo gỡ kịp thời các khó khăn, vướng mắc mang tính liên ngành, các điểm nghẽn vượt thẩm quyền của các bộ, ngành, địa phương.

b) Thường trực Ban Chỉ đạo

Chịu trách nhiệm chỉ đạo, điều hành trực tiếp, thường xuyên quá trình tổ chức thực hiện Kế hoạch; tổ chức giao ban định kỳ với Cơ quan Thường trực Ban Chỉ đạo an toàn, an ninh mạng quốc gia và các cơ quan liên quan trong việc hướng dẫn, đôn đốc, kiểm tra, giám sát tiến độ, tháo gỡ khó khăn, vướng mắc, bảo đảm Kế hoạch được triển khai đồng bộ, thống nhất, hiệu quả trong hệ thống chính trị.

c) Đảng uỷ Quốc hội, Đảng uỷ Chính phủ, Đảng uỷ Mặt trận Tổ quốc, các đoàn thể Trung ương

- Chỉ đạo các cơ quan liên quan rà soát, sửa đổi, bổ sung kịp thời ban hành các văn bản luật, văn bản hướng dẫn; tổ chức triển khai thực hiện các nhiệm vụ được giao và chủ động hướng dẫn, xử lý các vấn đề phát sinh theo chức năng, nhiệm vụ, thẩm quyền và lĩnh vực quản lý. **Nhiệm vụ thường xuyên.**

- Chỉ đạo thực hiện việc kết nối, liên thông các hệ thống thông tin phục vụ hoạt động và chỉ đạo, điều hành (hệ thống quản lý văn bản và hồ sơ công việc, hệ thống thông tin báo cáo, hệ thống họp trực tuyến...) của các khối cơ quan Đảng, Quốc hội, Chính phủ, Mặt trận Tổ quốc và các tổ chức chính trị - xã hội, Toà án nhân dân tối cao, Viện Kiểm sát nhân dân tối cao, bảo đảm an toàn và bảo mật thông tin. **Hoàn thành trong tháng 4/2026.**

- Chỉ đạo việc ban hành các quy định ưu tiên sử dụng sản phẩm, dịch vụ an ninh mạng, an toàn thông tin "Make in Vietnam" đáp ứng yêu cầu bảo đảm an ninh mạng, bảo mật dữ liệu và an toàn thông tin bảo vệ an ninh mạng cho các bộ, ngành, địa phương. **Hoàn thành trong tháng 4/2026.**

d) Đảng uỷ Công an Trung ương

- Chịu trách nhiệm trước Chính phủ thực hiện thống nhất quản lý nhà nước về an ninh mạng, bảo mật thông tin, an ninh dữ liệu (*trừ lĩnh vực quân sự, quốc phòng và cơ yếu*).

- Chỉ đạo Bộ Công an thực hiện các nhiệm vụ sau:

+ Giữ vai trò cơ quan thường trực về vấn đề bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu.

+ Rà soát, sửa đổi, bổ sung Luật Hình sự, pháp luật về xử lý vi phạm hành chính đủ sức răn đe, phòng ngừa xã hội và căn cứ xử lý các hành vi chưa được quy định; sửa đổi, bổ sung các quy định của pháp luật để phòng ngừa, đấu tranh, ngăn chặn và xử lý triệt để, kịp thời các hành vi vi phạm pháp luật trên không gian mạng. **Hoàn thành trước tháng 3/2027**.

+ Tập trung nâng cao năng lực của Trung tâm An ninh mạng quốc gia thuộc Bộ Công an; kết nối, chia sẻ dữ liệu giám sát, cảnh báo an ninh mạng đến các hệ thống thông tin quan trọng thuộc danh mục được ưu tiên bảo vệ của hệ thống chính trị từ cấp độ 3 trở lên (trừ các hệ thống thông tin trong lĩnh vực quân sự, quốc phòng và cơ yếu); thiết lập kênh kết nối trao đổi thông tin, dữ liệu phục vụ giám sát, điều phối ứng cứu, khắc phục sự cố an toàn thông tin, an ninh mạng (thuộc phạm vi quản lý). **Hoàn thành trong tháng 6/2026.**

+ Đẩy nhanh tiến độ xây dựng, vận hành Hệ thống phòng vệ mạng quốc gia trở thành nền tảng dùng chung trong Khung kiến trúc tổng thể quốc gia số nhằm bảo vệ an ninh mạng vòng ngoài cho các hệ thống thông tin, tài nguyên trọng yếu trên Internet của các cơ quan ban, bộ, ngành, địa phương, cơ quan, doanh nghiệp Việt Nam. **Triển khai trong năm 2026 và hoàn thành trong tháng 3/2027.**

+ Chủ trì, phối hợp với Bộ Quốc phòng, Bộ Khoa học và Công nghệ, Ban Cơ yếu Chính phủ và các Bộ, ngành, địa phương: *(i)* Sửa đổi TCVN 14423: 2025 về An ninh mạng - Yêu cầu đối với hệ thống thông tin mạng quan trọng trên cơ sở hợp nhất với TCVN 11923: 2017 theo thủ tục rút gọn cho phù hợp các cấp độ hệ thống thông tin theo Luật An ninh mạng 2025, **hoàn thành trước tháng 6/2026**. ***(ii)*** Xây dựng, ban hành quy định, hướng dẫn triển khai TCVN mới, định kỳ hàng năm thực hiện kiểm tra, đánh giá việc áp dụng TCVN, **hoàn thành trong tháng 8/2026.** ***(iii)*** Tổ chức chiến dịch truyền thông sâu rộng trên truyền hình, báo chí, mạng xã hội kết hợp cảnh báo trực tiếp qua nhà mạng, ngân hàng và nền tảng số; phổ cập kỹ năng an toàn số cho người dân thông qua chương trình giáo dục, tập huấn cộng đồng và tài liệu hướng dẫn trực tuyến; xây dựng hệ thống tiếp nhận, xử lý phản ánh 24/7 liên thông giữa cơ quan chức năng, tổ chức doanh nghiệp và người dân nhằm ngăn chặn kịp thời các hình thức lừa đảo trực tuyến. **Hoàn thành trong tháng 4/2026.**

+ Chủ trì, phối hợp Bộ Khoa học và Công nghệ, Bộ Quốc phòng và các cơ quan liên quan: ***(i)*** Ban hành Khung quản trị rủi ro an ninh mạng quốc gia; ban hành hướng dẫn về quản lý rủi ro an ninh mạng để các bộ, ngành, địa phương nghiên cứu, chuẩn bị nguồn lực thực hiện. **Hoàn thành trước tháng 12/2026.** ***(ii)*** Xây dựng chỉ số đảm bảo an ninh mạng làm cơ sở đánh giá năng lực bảo đảm an ninh mạng của các cơ quan, các bộ, ngành, địa phương, tổ chức, doanh nghiệp hằng năm; xếp hạng các bộ, ngành, tỉnh, thành phố trong phát triển khoa học, công nghệ, chuyển đổi số. **Hoàn thành trước tháng 6/2026.**

+ Chủ trì, phối hợp Bộ Khoa học và Công nghệ huy động các nguồn lực xã hội nghiên cứu, phát triển nền tảng điều hành và quản trị hạ tầng điện toán

đám mây do Việt Nam làm chủ đáp ứng các yêu cầu an ninh mạng; là sản phẩm chiến lược nhằm bảo đảm chủ quyền số quốc gia; ưu tiên phục vụ lưỡng dụng, kết hợp chặt chẽ giữa bảo đảm an ninh và phát triển kinh tế, sẵn sàng cung cấp để triển khai hạ tầng số cho các cơ quan trong hệ thống chính trị từ Trung ương đến cơ sở (trừ hệ thống thông tin quân sự, quốc phòng, cơ yếu). **Hoàn thành trước 12/2026.**

+ Chủ trì, phối hợp với Bộ Quốc phòng, Bộ Tài chính, Bộ Khoa học và Công nghệ và các cơ quan liên quan rà soát, sửa đổi, bổ sung các quy định pháp luật để quy định an ninh mạng, bảo mật thông tin, an ninh dữ liệu là thành phần bắt buộc trong mọi dự án công nghệ thông tin; bảo đảm tỉ lệ kinh phí bình quân chi cho các sản phẩm, dịch vụ an ninh mạng, bảo mật thông tin, an ninh dữ liệu đạt tối thiểu 15% trong tổng kinh phí triển khai đề án, dự án, chương trình, kế hoạch đầu tư, ứng dụng, phát triển công nghệ thông tin, bảo đảm hiệu quả, đúng quy định, tránh lãng phí. **Hoàn thành trong tháng 4/2026.**

+ Xây dựng cơ chế hậu kiểm và đánh giá hiệu quả việc thực hiện chỉ tiêu tối thiểu 15% ngân sách cho an ninh mạng; trong đó ưu tiên sử dụng cho các sản phẩm "Make in Vietnam" đã qua kiểm định, đánh giá chất lượng **Hoàn thành trong tháng 12/2026.**

+ Chủ trì, phối hợp Viện Kiểm sát nhân dân tối cao, Toà án nhân dân tối cao rà soát, sửa đổi, bổ sung các quy định của pháp luật yêu cầu tổ chức, doanh nghiệp cung cấp dịch vụ tài chính, ngân hàng, viễn thông, Internet, trung gian thanh toán, dịch vụ trên không gian mạng trong nước thực hiện kết nối kỹ thuật, cung cấp thông tin, dữ liệu, chứng cứ đầy đủ, kịp thời qua phương thức điện tử cho cơ quan chức năng, cắt giảm thủ tục hành chính nhằm bảo đảm thời gian tính phục vụ phòng ngừa, đấu tranh, ngăn chặn và xử lý các hành vi vi phạm pháp luật trên không gian mạng. **Hoàn thành trong tháng 12/2026.**

+ Chủ trì, phối hợp với Bộ Giáo dục và Đào tạo và các đơn vị có liên quan xây dựng: (1) Các khoá đào tạo thực tế về công tác bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu cho cán bộ chuyên trách an ninh mạng của các đơn vị, địa phương. (2) Triển khai đào tạo, đặc biệt là phối hợp với các cơ quan truyền thông, báo chí (Chương trình, chuyện mục trên khung giờ "vàng" của Đài Truyền hình Việt Nam, Đài Tiếng nói Việt Nam...), mạng xã hội nhằm phổ biến kiến thức an ninh mạng trên nền tảng "Bình dân học vụ số" cho người sử dụng mạng. **Nhiệm vụ thường xuyên.**

+ Triển khai chương trình đánh giá tín nhiệm mạng đối với các tổ chức, cá nhân có ảnh hưởng trên không gian mạng; củng cố lòng tin, trách nhiệm của người dân khi hoạt động, tương tác, làm việc trên không gian mạng. **Nhiệm vụ thường xuyên.**

+ Triển khai hiệu quả, có thực chất Công ước Hà Nội về chống tội phạm mạng năm 2025. **Nhiệm vụ thường xuyên.**

đ) Quân uỷ Trung ương

- Chịu trách nhiệm toàn diện trước Bộ Chính trị, Ban Bí thư về công tác bảo đảm an ninh mạng, mật mã, bảo mật thông tin trong lĩnh vực quân sự, quốc phòng, cơ yếu thuộc phạm vi quản lý của Bộ Quốc phòng.

- Chỉ đạo công tác bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu theo phạm vi quản lý, chức năng, nhiệm vụ được giao.

- Chỉ đạo Bộ Quốc phòng thực hiện các nhiệm vụ sau:

+ Theo chức năng, nhiệm vụ được giao và trong lĩnh vực thuộc phạm vi quản lý, tổ chức triển khai các hoạt động trong công tác bảo đảm, giám sát an ninh mạng, bảo mật thông tin, an ninh dữ liệu đối với các hệ thống thông tin quân sự, quốc phòng, cơ yếu do Bộ Quốc phòng và Ban Cơ yếu Chính phủ quản lý (bao gồm cả hệ thống thông tin, dữ liệu thuộc các cơ quan, đơn vị, tổ chức, doanh nghiệp có hoạt động liên quan đến lĩnh vực quân sự, quốc phòng). **Nhiệm vụ thường xuyên**.

+ Nâng cao năng lực Trung tâm giám sát Không gian mạng và lực lượng chuyên trách an ninh mạng thuộc Bộ Quốc phòng. **Hoàn thành trước tháng 6/2026**.

+ Xây dựng và ban hành các tiêu chuẩn, quy chuẩn kỹ thuật cho sản phẩm, dịch vụ an ninh mạng trong phạm vi quản lý. **Hoàn thành trước tháng 12/2027.**

+ Phối hợp với Bộ Công an xây dựng cơ chế kết nối, chia sẻ thông tin cảnh báo sớm về an ninh mạng giữa Trung tâm An ninh mạng quốc gia với Trung tâm giám sát Không gian mạng (Bộ Quốc phòng) theo chức năng, nhiệm vụ được giao. **Hoàn thành trong tháng 6/2026**.

+ Phối hợp với các cơ quan chủ quản hệ thống thông tin quan trọng quốc gia tăng cường nguồn lực, hỗ trợ bảo vệ hệ thống thông tin, an ninh mạng, bảo mật thông tin và an ninh dữ liệu. **Nhiệm vụ thường xuyên.**

+ Bộ trưởng Bộ Quốc phòng chỉ đạo Ban Cơ yếu Chính phủ: **(i)** Chủ trì, phối hợp với Bộ Công an, Bộ Khoa học và Công nghệ, cơ quan liên quan xây dựng Khung kiến trúc hạ tầng mật mã quốc gia. **Hoàn thành trong tháng 3/2026. (ii)** Bảo đảm hạ tầng mật mã quốc gia hoạt động ổn định, an toàn phục vụ bảo mật, trao đổi dữ liệu bí mật nhà nước từ Trung ương đến 100% cấp xã. **Nhiệm vụ thường xuyên. (iii)** Chủ trì, phối hợp với Bộ Công an, Bộ Khoa học và Công nghệ xây dựng các tiêu chuẩn, quy chuẩn kỹ thuật về mật mã dân sự để bảo vệ an ninh mạng. **Nhiệm vụ thường xuyên.**

e) Đảng uỷ Bộ Khoa học và Công nghệ

Chỉ đạo Bộ Khoa học và Công nghệ thực hiện các nhiệm vụ sau:

- Chủ trì, phối hợp Bộ Công an, Bộ Quốc phòng và các bộ, ngành, địa phương liên quan rà soát, trình cấp có thẩm quyền xem xét, điều chỉnh quy hoạch hạ tầng thông tin tổng thể từ Trung ương đến cơ sở theo hướng tập trung

các máy chủ về các trung tâm dữ liệu đạt chuẩn, đủ điều kiện để triển khai đầy đủ các biện pháp bảo vệ an ninh mạng theo quy định. **Hoàn thành trong tháng 6/2026.**

- Chủ trì, phối hợp cơ quan liên quan, ban hành tiêu chuẩn quốc gia cho sản phẩm, dịch vụ an ninh mạng thuộc các lĩnh vực then chốt (*Cloud, Chính phủ số, IoT/OT, AI, Blockchain, viễn thông*), phối hợp Bộ Công an sửa đổi TCVN 14423: 2025 cho phù hợp với các cấp độ hệ thống thông tin theo Luật An ninh mạng số 116/2025/QH15. **Hoàn thành trước tháng 12/2026.**

- Chủ trì, phối hợp với các cơ quan liên quan xây dựng, trình cấp có thẩm quyền ban hành cơ chế, chính sách đặc thù thu hút và hỗ trợ các doanh nghiệp công nghệ trong nước, tạo điều kiện thuận lợi để làm chủ các công nghệ cốt lõi và phát triển các sản phẩm "Make in Vietnam" có tính đột phá, đủ sức cạnh tranh trên thị trường quốc tế. **Hoàn thành trong tháng 4/2026**.

g) Đảng uỷ Bộ Giáo dục và Đào tạo

Chỉ đạo Bộ Giáo dục và Đào tạo thực hiện các nhiệm vụ sau:

- Chủ trì rà soát, xây dựng chương trình đào tạo chuyên sâu về an ninh mạng và công nghệ lõi; phối hợp với Bộ Công an, Bộ Quốc phòng, Ban Cơ yếu Chính phủ và các đơn vị có liên quan xây dựng các khoá đào tạo thực tế về công tác bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu cho cán bộ chuyên trách an ninh mạng của các đơn vị, địa phương. **Nhiệm vụ thường xuyên**.

- Chủ trì, phối hợp Bộ Công an, Bộ Quốc phòng xây dựng và triển khai các chương trình đào tạo, tập huấn, bồi dưỡng kiến trức, kỹ năng sư phạm về bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trên nền tảng "Bình dân học vụ số". **Nhiệm vụ thường xuyên.**

- Chủ trì xây dựng và triển khai "Khung Năng lực số và An toàn mạng Toàn diện" trong chương trình giáo dục phổ thông (tích hợp các kỹ năng thực hành (như nhận diện lừa đảo, quản lý danh tính số, ứng phó với bắt nạt trên mạng) vào các môn học chính khoá, giúp hình thành văn hoá số an toàn từ sớm cho thế hệ trẻ). **Hoàn thành Khung chương trình trong tháng 6/2026.**

h) Đảng uỷ Bộ Tài chính

Chỉ đạo Bộ Tài chính thực hiện các nhiệm vụ sau:

- Chủ trì, phối hợp với Bộ, ngành bảo đảm kinh phí đầu tư từ ngân sách trung ương cho hoạt động an ninh mạng, bảo mật thông tin và an ninh dữ liệu cho các cơ quan trung ương. Hướng dẫn các cơ quan tài chính địa phương bảo đảm kinh phí đầu tư từ ngân sách địa phương cho các hoạt động an ninh mạng, bảo mật thông tin và an ninh dữ liệu tại địa phương. **Nhiệm vụ thường xuyên.**

- Chủ trì, phối hợp với các cơ quan liên quan điều chỉnh đồng bộ các quy định về tài chính, công sản, ngân sách, đấu thầu có liên quan để tạo thuận lợi trong quá trình triển khai thực tiễn, đáp ứng yêu cầu nhiệm vụ và đặc thù vòng đời của sản phẩm giải pháp an ninh mạng thường ngắn hơn quy định về khấu hao công sản. **Hoàn thành trong tháng 3/2026.**

i) Đảng uỷ Bộ Ngoại giao: Chỉ đạo Bộ Ngoại giao chủ trì, phối hợp chặt chẽ với Bộ Quốc phòng, Bộ Công an, Bộ Khoa học và Công nghệ trong việc tham gia, đóng góp tại các cơ chế đa phương như Liên hợp quốc, ASEAN về các nội dung liên quan đến an ninh mạng và các công nghệ mới. **Nhiệm vụ thường xuyên**.

k) Ban Tuyên giáo và Dân vận Trung ương: Chủ trì, phối hợp với các cơ quan liên quan trong thực hiện công tác tuyên truyền, phổ biến giáo dục pháp luật về bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu; giáo dục kỹ năng bảo vệ dữ liệu cá nhân, phòng, chống tội phạm lừa đảo, chiếm đoạt tài sản trên không gian mạng. **Nhiệm vụ thường xuyên.**

m) Các bộ, cơ quan, địa phương

- Kiện toàn tiểu ban chỉ đạo an ninh mạng tại các Bộ, ngành, địa phương, trong đó trưởng tiểu ban là bí thư tỉnh uỷ, thành uỷ, bộ trưởng, thủ trưởng các cơ quan, đơn vị. **Hoàn thành trong tháng 02/2026.**

- Chủ trì, phối hợp với các cơ quan liên quan rà soát, đánh giá và củng cố lại Hệ thống giám sát an ninh mạng tại các Bộ, ngành, địa phương; công an tỉnh, thành phố chủ trì, phối hợp với Sở Khoa học và Công nghệ thực hiện công tác giám sát, điều phối ứng phó xử lý sự cố tại địa phương. **Hoàn thành trong tháng 3/2026.**

- Các Bộ, ngành, địa phương có trung tâm dữ liệu dùng riêng, trực tiếp quản lý, vận hành các hệ thống thông tin trọng yếu xây dựng, hình thành Trung tâm giám sát an ninh mạng tập trung, đảm bảo hoạt động giám sát và sẵn sàng ứng phó với các nguy cơ tấn công mạng, đồng thời có thể chia sẻ dữ liệu giám sát với hệ thống giám sát an ninh mạng quốc gia; giao Bộ trưởng chỉ đạo đơn vị chuyên trách về công nghệ thông tin chủ trì, phối hợp với Bộ Công an và các cơ quan xây dựng phương án ứng cứu sự cố an ninh mạng cho hệ thống thuộc phạm vi quản lý, thực hiện công tác giám sát, điều phối, ứng phó xử lý sự cố *(trừ các hệ thống thông tin trong lĩnh vực quân sự, quốc phòng và cơ yếu)*. **Hoàn thành trong tháng 5/2026**.

- Chủ trì, phối hợp với Bộ Công an, Bộ Quốc phòng và Ban Cơ yếu Chính phủ (theo phạm vi quản lý) tổ chức rà soát, đánh giá tổng thể về an ninh mạng, bảo mật thông tin và an ninh dữ liệu đối với các cơ sở dữ liệu quốc gia, chuyên ngành, hệ thống thông tin và nguồn nhân lực. **Hoàn thành trong tháng 6/2026.**

- Chỉ đạo các cơ quan, đơn vị huy động mọi nguồn lực để khắc phục ngay những lỗ hổng bảo mật trong các hệ thống thông tin. **Hoàn thành trong tháng 4/2026**.

- Phối hợp với các cơ quan liên quan để tổ chức thẩm định, phê duyệt cấp độ đối với toàn bộ các hệ thống thông tin trọng yếu do mình trực tiếp quản lý, vận hành. Đối với hạ tầng và các hệ thống thông tin đang xây dựng hoặc sẽ triển khai trong thời gian tới, yêu cầu bắt buộc phải thực hiện phê duyệt cấp độ an toàn thông tin trước khi đưa vào vận hành chính thức. Đối với các hệ thống thông tin và hạ tầng hiện đang sử dụng, cần khẩn trương rà soát, đánh giá và

thực hiện phê duyệt cấp độ an toàn thông tin theo đúng quy định. **Hoàn thành trong tháng 4/2026.**

- Phối hợp Bộ Công an thực hiện thiết lập kênh kết nối trao đổi thông tin, dữ liệu phục vụ giám sát, điều phối ứng cứu, khắc phục sự cố an toàn thông tin, an ninh mạng theo hướng dẫn của lực lượng chuyên trách bảo vệ an ninh mạng Bộ Công an theo quy định *(trừ các hệ thống thông tin trong lĩnh vực quân sự, quốc phòng và cơ yếu)*. **Hoàn thành trong tháng 4/2026.** Thực hiện báo cáo về sự cố trong vòng 24 giờ nếu xảy ra và tuân theo sự điều phối ứng phó sự cố của lực lượng chuyên trách bảo vệ an ninh mạng Bộ Công an theo quy định. **Nhiệm vụ thường xuyên**.

- Phối hợp Bộ Công an sửa đổi, bổ sung các quy định pháp luật về bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu và danh mục bảo vệ bí mật nhà nước để phù hợp với quy định mới tại Luật An ninh mạng, Luật Bảo vệ bí mật nhà nước. **Hoàn thành trong tháng 3/2026.**

- Triển khai tổng thể các giải pháp giám sát, bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu cho các hệ thống thông tin trong phạm vi quản lý. **Hoàn thành trong tháng 4/2026.**

- Triển khai mô hình bảo đảm an toàn thông tin "4 lớp" gồm: (1) Lực lượng tại chỗ chịu trách nhiệm vận hành, giám sát và ứng cứu ban đầu khi sự cố xảy ra. (2) Hệ thống hoặc dịch vụ giám sát 24/7, giúp phát hiện sớm các nguy cơ. (3) Đơn vị độc lập thực hiện kiểm tra, đánh giá định kỳ để đảm bảo khách quan và minh bạch. (4) Kết nối, chia sẻ thông tin với hệ thống giám sát an ninh mạng quốc gia, bảo đảm sự phối hợp liên thông trên phạm vi toàn quốc (trừ các hệ thống thông tin quân sự, quốc phòng, cơ yếu). **Hoàn thành trong tháng 4/2026.**

- Bộ Quốc phòng, Bộ Công an theo chức năng, nhiệm vụ chủ trì, phối hợp với Bộ Khoa học và Công nghệ, các cơ quan liên quan nghiên cứu xây dựng đề án về phát triển mã hoá kháng lượng tử và khuyến khích việc xã hội hoá hoạt động nghiên cứu, phát triển ứng dụng mật mã dân sự, trình Thủ tướng Chính phủ xem xét quyết định **trong tháng 3/2026.**

- Bộ Công an, Bộ quốc phòng theo phạm vi quản lý, chức năng, nhiệm vụ được giao, chủ trì, phối hợp với Cơ quan Thường trực Ban Chỉ đạo Trung ương chuẩn bị tài liệu, báo cáo phục vụ các cuộc họp, làm việc của Thường trực Ban Chỉ đạo Trung ương với các cơ quan liên quan về các nội dung, nhiệm vụ theo Kế hoạch này.

- Phải bảo đảm tích hợp đầy đủ yêu cầu về an toàn ninh mạng, bảo mật thông tin và an ninh dữ liệu trong toàn bộ quá trình thiết kế, thẩm định và triển khai khi xây dựng, cập nhật hoặc hoàn thiện Khung kiến trúc tổng thể quốc gia số.

n) Người đứng đầu các cơ quan, tổ chức trong hệ thống chính trị từ Trung ương đến địa phương có trách nhiệm lãnh đạo, chỉ đạo, kiểm tra và đôn đốc thực hiện công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ

liệu. Chịu trách nhiệm trực tiếp và toàn diện nếu để xảy ra sự cố an ninh mạng nghiêm trọng, đặc biệt là lộ, lọt bí mật nhà nước do yếu tố chủ quan, thiếu trách nhiệm hoặc không tuân thủ quy định. Đưa kết quả đánh giá chỉ số bảo đảm an ninh mạng của các cơ quan, tổ chức vào tiêu chí đánh giá tín nhiệm, năng lực của cán bộ, nhất là đối với người đứng đầu, để phục vụ công tác xếp loại hàng năm. Triển khai chương trình đánh giá tín nhiệm mạng đối với các tổ chức, cá nhân có ảnh hưởng trên không gian mạng nhằm củng cố lòng tin số của người dân trong quá trình hoạt động, tương tác và làm việc trên không gian mạng. **Nhiệm vụ thường xuyên.**

o) Hiệp hội An ninh mạng quốc gia: Xây dựng mạng lưới liên kết các chuyên gia an ninh mạng trong nước và nước ngoài tham gia hỗ trợ công tác bảo đảm an ninh mạng. Mở rộng Liên minh ứng phó, khắc phục sự cố an ninh mạng quốc gia.

p) Các doanh nghiệp lớn tham gia chủ trì, đồng hành trong hoạt động chuyển đổi số tại các cơ quan, đơn vị, bộ, ngành, địa phương có trách nhiệm phối hợp chặt chẽ với cơ quan, đơn vị chủ quan trong việc thực hiện đầy đủ các quy định của pháp luật về bảo đảm an ninh mạng, an toàn thông tin và bảo vệ dữ liệu trong quá trình thiết kế, triển khai, vận hành hệ thống thông tin, nền tảng số, dịch vụ số; tuân thủ tiêu chuẩn, quy chuẩn kỹ thuật quốc gia về an toàn thông tin mạng, bảo vệ dữ liệu cá nhân; chịu trách nhiệm trước cơ quan chủ quản, cơ quan có thẩm quyền nếu để xảy ra sự cố, rò rỉ, mất an toàn thông tin do lỗi chủ quan hoặc vi phạm quy trình. Các doanh nghiệp cung cấp dịch vụ viễn thông, Internet trong nước phải phát huy vai trò là tuyến đầu phòng thủ và có trách nhiệm tuân thủ quy định trong công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu.

2. Kinh phí thực hiện

- Nguồn kinh phí thực hiện Kế hoạch được bảo đảm từ ngân sách nhà nước theo phân cấp, đồng thời lồng ghép trong các chương trình, đề án, dự án có liên quan và huy động thêm các nguồn vốn hợp pháp khác.

- Ưu tiên bố trí ngân sách cho các nhiệm vụ cấp bách. Áp dụng linh hoạt các cơ chế tài chính đặc thù đã được cấp có thẩm quyền phê duyệt nhằm đáp ứng yêu cầu tiến độ thực hiện.

- Việc triển khai các nội dung, nhiệm vụ, giải pháp của Kế hoạch bảo đảm thiết thực, hiệu quả, tránh trùng lặp, lãng phí, tiêu cực.

3. Chế độ thông tin, báo cáo

Các cơ quan, đơn vị, địa phương thực hiện cập nhật báo cáo định kỳ hằng tháng (trước ngày 25 hằng tháng) trên Hệ thống thông tin giám sát, đánh giá việc thực hiện Nghị quyết số 57-NQ/TW (https: //theodoinq.dcs.vn).

4. Tổng kết, đánh giá và khen thưởng kỷ luật

- Gắn kết quả thực hiện Kế hoạch với đánh giá, xếp loại mức độ hoàn thành nhiệm vụ của tập thể và cá nhân, đặc biệt là người đứng đầu.

- Kịp thời biểu dương, khen thưởng các tập thể, cá nhân có thành tích xuất sắc, các mô hình hay, cách làm sáng tạo; đồng thời xem xét, xử lý nghiêm các trường hợp không hoàn thành nhiệm vụ, thiếu trách nhiệm, gây ảnh hưởng đến các mục tiêu chung của Kế hoạch.

- Các cấp uỷ, tổ chức đảng, các cơ quan, đơn vị triển khai thực hiện nghiêm túc Kế hoạch này.

K/T TRƯỞNG BAN
PHÓ TRƯỞNG BAN

Trần Cẩm Tú

Nơi nhận:
- Bộ Chính trị, Ban Bí thư (để báo cáo),
- Đồng chí Tổng Bí thư, Trưởng Ban Chỉ đạo (để báo cáo),
- Thành viên Ban Chỉ đạo Trung ương,
- Các đảng uỷ trực thuộc Trung ương,
- Các ban đảng Trung ương,
- Các Đảng uỷ bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ; uỷ ban nhân dân các tỉnh, thành phố (để thực hiện),
- Các tỉnh uỷ, thành uỷ (để thực hiện),
- Mặt trận Tổ quốc và các đoàn thể Trung ương (để thực hiện),
- Toà án nhân dân tối cao (để thực hiện),
- Viện Kiểm sát nhân dân tối cao (để thực hiện),
- Thường trực Tổ Giúp việc Ban Chỉ đạo (để thực hiện),
- Văn phòng Trung ương Đảng,
- Lưu Ban Chỉ đạo Trung ương.

TỈNH ỦY THANH HÓA
*
Số 152-BS/TU

Nơi nhận:
- Các đ/c Thường vụ Tỉnh ủy,
- Các đảng bộ trực thuộc,
- Các ban, sở, ngành, MTTQ, đoàn thể cấp tỉnh,
- Lưu Văn phòng Tỉnh uỷ.

SAO Y

Thanh Hoá, ngày 20 tháng 03 năm 2026

T/L. BAN THƯỜNG VỤ
CHÁNH VĂN PHÒNG

Nguyễn Lợi Đức