SAO Y; Tỉnh ủy Hưng Yên; Thời gian ký: 2026-01-29T16:22:41+07:00

BAN BÍ THƯ TRUNG ƯƠNG ĐẢNG
BAN BÍ THƯ TRUNG ƯƠNG ĐẢNG
27-01-2026 15:18:51 +07:00

BAN CHẤP HÀNH TRUNG ƯƠNG
*
Số 57-CT/TW

ĐẢNG CỘNG SẢN VIỆT NAM

Hà Nội, ngày 31 tháng 12 năm 2025

CHỈ THỊ
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

Thời gian qua, thực hiện chủ trương, các nghị quyết, kết luận của Ban Chấp hành Trung ương Đảng, Bộ Chính trị, Ban Bí thư, công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu đã được các cấp uỷ, tổ chức đảng quan tâm lãnh đạo, chỉ đạo; nhận thức về tầm quan trọng của an ninh mạng được nâng lên; hành lang pháp lý từng bước được hoàn thiện; năng lực kỹ thuật bảo đảm an ninh mạng của một số cơ quan được tăng cường; hoạt động hợp tác quốc tế lĩnh vực an ninh mạng đạt được dấu ấn quan trọng, góp phần đưa chỉ số an ninh mạng toàn cầu của Việt Nam vươn lên thứ hạng cao trên các bảng xếp hạng quốc tế. An ninh mạng, bảo mật thông tin, an ninh dữ liệu đã được đặc biệt coi trọng trong quá trình chuyển đổi số quốc gia, triển khai Chính phủ điện tử, góp phần nâng cao hiệu lực, hiệu quả hoạt động của các cơ quan, tổ chức trong hệ thống chính trị sau sắp xếp, sáp nhập, hợp nhất, điều chỉnh địa giới hành chính và thực hiện mô hình chính quyền địa phương 2 cấp.

Bên cạnh những kết quả đạt được, công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu vẫn còn nhiều tồn tại, hạn chế: Công tác quản lý nhà nước chưa theo kịp yêu cầu thực tiễn, tổ chức thực hiện chồng chéo, thiếu đồng bộ; nhận thức của một bộ phận lãnh đạo, cán bộ, đảng viên và Nhân dân về an ninh mạng, bảo mật thông tin còn chưa đầy đủ và sâu sắc; còn tình trạng một số hệ thống thông tin chưa đủ điều kiện an ninh mạng theo quy định, nhưng đã được đưa vào sử dụng, tạo ra các rủi ro về an ninh mạng, buộc phải đầu tư bổ sung để bảo đảm tuân thủ các quy định của pháp luật, các điều kiện về an ninh mạng; nguồn nhân lực chất lượng cao còn thiếu; ngân sách dành cho an toàn, bảo mật thông tin chưa đáp ứng yêu cầu; hạ tầng số chưa đồng bộ, một số hệ thống được đầu tư manh mún chưa bảo đảm các tiêu chuẩn an ninh mạng tối thiểu; mức độ tự chủ về công nghệ, sản phẩm an ninh mạng chưa cao.

Dự báo tình hình an ninh mạng, bảo mật thông tin, an ninh dữ liệu trên thế giới và trong nước có nhiều diễn biến phức tạp, khó lường. Trong bối cảnh dữ liệu trở thành tài nguyên chiến lược, trí tuệ nhân tạo phát triển nhanh chóng,

không gian mạng trở thành không gian tác chiến mới, công tác bảo đảm an ninh mạng, an ninh dữ liệu, bảo mật thông tin không chỉ là nhiệm vụ kỹ thuật mà là vấn đề an ninh quốc gia, chủ quyền quốc gia, ổn định chính trị, xã hội và năng lực cạnh tranh quốc gia. Việt Nam phải đối mặt với những thách thức nghiêm trọng đe doạ an ninh quốc gia, trật tự, an toàn xã hội. Đồng thời, công cuộc chuyển đổi số đặt ra yêu cầu cấp bách đối với công tác bảo đảm an ninh thông tin, an ninh mạng quốc gia trong tình hình mới.

Tại Nghị quyết số 57-NQ/TW, ngày 22/12/2024 của Bộ Chính trị đã đưa ra một số định hướng, mục tiêu, yêu cầu đối với công tác bảo đảm an toàn, an ninh mạng, bảo đảm chủ quyền quốc gia trên không gian mạng.

Trước yêu cầu, nhiệm vụ đặt ra trong giai đoạn mới, bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu là yêu cầu cấp thiết nhằm kiến tạo một không gian mạng an toàn, tin cậy, thúc đẩy mạnh mẽ sự phát triển khoa học, công nghệ, đổi mới sáng tạo, chuyển đổi số quốc gia, Ban Bí thư yêu cầu các cấp uỷ, tổ chức đảng tập trung lãnh đạo, chỉ đạo thực hiện tốt một số nhiệm vụ, giải pháp trọng tâm sau:

1. Tăng cường sự lãnh đạo của Đảng, nâng cao nhận thức, trách nhiệm của cả hệ thống chính trị và toàn dân về an ninh mạng, bảo mật thông tin, an ninh dữ liệu

a) Quán triệt sâu sắc quan điểm bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu là nhiệm vụ trọng yếu, thường xuyên, cấp bách; là trách nhiệm của cả hệ thống chính trị và toàn dân, đặt dưới sự lãnh đạo trực tiếp, toàn diện của Đảng, sự quản lý tập trung, thống nhất của Nhà nước. Lực lượng Công an nhân dân, Quân đội nhân dân đóng vai trò chủ chốt. Huy động sức mạnh tổng hợp của toàn dân, xây dựng thế trận an ninh nhân dân gắn với thế trận quốc phòng toàn dân trên không gian mạng.

b) Chuyển dịch tư duy chiến lược từ "Phòng thủ bị động" sang "Phòng thủ chủ động", "Phòng thủ tích cực", xây dựng "Thế trận an ninh mạng chủ động, toàn diện"; những nguy cơ, thách thức về an ninh mạng, bảo mật thông tin, an ninh dữ liệu phải được nhận diện và xử lý từ sớm, từ xa, sẵn sàng có các biện pháp phòng vệ tương xứng để răn đe, vô hiệu hoá các nguy cơ, bảo vệ lợi ích quốc gia - dân tộc.

c) Quán triệt phương châm "Tự chủ, tự lực, tự cường" trong xây dựng tiềm lực an ninh mạng. Tập trung phát triển, khai thác, sử dụng hệ sinh thái sản phẩm, dịch vụ an ninh mạng Việt Nam, ưu tiên làm chủ công nghệ lõi, giải pháp bảo mật tiên tiến, ứng dụng mạnh mẽ trí tuệ nhân tạo, công nghệ mới vào lĩnh vực an ninh mạng, coi đây là những nhiệm vụ chiến lược để bảo vệ vững chắc

chủ quyền quốc gia trên không gian mạng. Áp dụng cơ chế đột phá, đặc thù, ưu đãi nhất trong lĩnh vực khoa học, công nghệ, đổi mới sáng tạo để phát triển hệ sinh thái sản phẩm, dịch vụ an ninh mạng, an ninh dữ liệu.

d) Bảo đảm an ninh mạng, an ninh dữ liệu là yếu tố nền tảng, yêu cầu bắt buộc ngay từ khâu quy hoạch, thiết kế, xây dựng, vận hành hệ thống thông tin. Hệ thống chưa bảo đảm an toàn, an ninh thì kiên quyết chưa đưa vào sử dụng. Thường xuyên rà soát, kiểm tra, đánh giá an ninh mạng đối với các hệ thống công nghệ thông tin. Việc thu thập, quản lý, khai thác dữ liệu số phải được bảo vệ ở mức độ cao nhất; tuyệt đối không để lộ, lọt bí mật nhà nước, dữ liệu nhạy cảm, kể cả trong quá trình thử nghiệm.

đ) Người đứng đầu cấp uỷ, chính quyền, cơ quan, đơn vị chịu trách nhiệm trực tiếp, toàn diện về công tác bảo đảm an ninh mạng, an ninh dữ liệu, bảo vệ bí mật nhà nước tại địa phương, đơn vị mình. Kết quả công tác này là một trong những tiêu chí quan trọng để đánh giá, xếp loại tổ chức, cán bộ, đảng viên, công chức, viên chức và người lao động hằng năm.

e) Đổi mới mạnh mẽ nội dung, hình thức tuyên truyền, giáo dục kiến thức, kỹ năng an ninh mạng; đưa nội dung này vào chương trình của hệ thống giáo dục quốc dân, chuyên đề trong Phong trào "Bình dân học vụ số" để xây dựng "thế hệ công dân số" văn minh, tuân thủ pháp luật. Triển khai đánh giá tín nhiệm mạng, phát triển cơ chế liên kết và hợp tác nhằm xây dựng một không gian mạng an toàn, tin cậy, thúc đẩy các giá trị nhân văn và nâng cao ý thức trách nhiệm bảo đảm an ninh không gian mạng đến mọi người dùng; phát động phong trào toàn dân bảo vệ an ninh mạng; phát huy trách nhiệm xã hội của cơ quan báo chí và người có uy tín trong việc định hướng dư luận, lan toả thông tin tích cực và đấu tranh với các thông tin xấu độc. Tập trung đào tạo, nâng cao năng lực, kỹ năng của lực lượng chuyên trách về an ninh mạng.

g) Triển khai hệ thống định danh và xác thực không gian mạng quốc gia; thống nhất định danh công dân, người dùng mạng xã hội, thuê bao viễn thông và tài nguyên Internet (tên miền, địa chỉ IP...). Kiên quyết xử lý triệt để tình trạng SIM "rác", tài khoản "ảo", nặc danh; áp dụng biện pháp xác thực danh tính bắt buộc đối với người dùng mạng xã hội và cơ chế kiểm soát độ tuổi để bảo vệ trẻ em trên không gian mạng.

2. Hoàn thiện thể chế, chính sách và nâng cao hiệu lực, hiệu quả quản lý nhà nước

a) Khẩn trương rà soát, sửa đổi, bổ sung, hoàn thiện, thống nhất, đồng bộ hệ thống pháp luật, cơ chế, chính sách về an ninh mạng, bảo mật thông tin, bảo vệ dữ liệu cá nhân, dữ liệu quốc gia, tiêu chuẩn, quy chuẩn kỹ thuật. Xây dựng chế tài xử lý nghiêm minh các hành vi vi phạm pháp luật trên không gian mạng.

b) Thống nhất đầu mối, phân định rõ trách nhiệm quản lý nhà nước bảo đảm hiệu lực, hiệu quả. Trong đó:

- *Về an ninh mạng:* Bộ Công an chịu trách nhiệm trước Chính phủ chủ trì quản lý nhà nước về an ninh mạng, bảo mật thông tin, an ninh dữ liệu xuyên suốt (từ thiết kế, tạo lập, triển khai đến vận hành) đối với các hệ thống thông tin, cơ sở dữ liệu của toàn hệ thống chính trị và quản lý hoạt động cung cấp sản phẩm, dịch vụ an ninh mạng đối với các hệ thống này (trừ hệ thống thông tin, cơ sở dữ liệu quân sự và cơ yếu trong phạm vi Bộ Quốc phòng quản lý).

- *Về mật mã và sản phẩm mật mã:* Bộ Công an, Bộ Quốc phòng, Ban Cơ yếu Chính phủ thực hiện trách nhiệm, phạm vi quản lý theo đúng quy định tại Luật An ninh mạng năm 2025.

c) Quy hoạch và phát triển hạ tầng số, hạ tầng dữ liệu quốc gia bảo đảm hiện đại, đồng bộ, an toàn. Thực hiện nghiêm quy định pháp luật yêu cầu hồ sơ thiết kế hệ thống thông tin, dự án chuyển đổi số phải có cấu phần an ninh mạng được thẩm định, phê duyệt trước khi đầu tư xây dựng.

d) Xây dựng Khung quản trị rủi ro an ninh mạng quốc gia theo tiêu chuẩn quốc tế; chuyển đổi tư duy từ quản lý kỹ thuật thuần tuý sang quản trị rủi ro toàn diện nhằm tăng tính chủ động phân bổ nguồn lực và giảm thiểu tổn thất. Xây dựng và áp dụng Bộ chỉ số đánh giá năng lực bảo đảm an ninh mạng để xếp hạng các bộ, ngành, địa phương, tổ chức. Hoàn thiện cơ chế trao đổi, chia sẻ thông tin và quy trình phối hợp ứng cứu sự cố giữa các cơ quan, tổ chức trong nước và quốc tế.

đ) Hoàn thiện hành lang pháp lý quản lý chặt chẽ hoạt động của các doanh nghiệp cung cấp dịch vụ trên không gian mạng (bao gồm cả dịch vụ xuyên biên giới). Quy định rõ trách nhiệm của các doanh nghiệp viễn thông, Internet, tài chính, ngân hàng trong việc bảo đảm an ninh hệ thống và phối hợp với cơ quan chức năng (Bộ Công an, Bộ Quốc phòng); thiết lập cơ chế kết nối kỹ thuật, cung cấp dữ liệu, chứng cứ điện tử nhanh chóng, kịp thời, bảo đảm "đúng, đủ, sạch, sống" để phục vụ công tác điều tra, xử lý tội phạm và bảo vệ chủ quyền quốc gia; đơn giản hoá thủ tục hành chính trong các tình huống khẩn cấp về an ninh mạng.

3. Tập trung đầu tư, hiện đại hoá hạ tầng, công nghệ và các giải pháp kỹ thuật bảo đảm an ninh mạng

a) Tập trung nguồn lực quốc gia nghiên cứu, phát triển và ứng dụng thuật toán mật mã kháng lượng tử để bảo vệ bí mật nhà nước, bảo đảm an ninh mạng trước thách thức về công nghệ giải mã sử dụng tính toán lượng tử; làm chủ các công nghệ lõi chiến lược như công nghệ mật mã, thiết kế và sản xuất chip bảo mật

"Make in Vietnam"; khuyến khích xã hội hoá đối với công tác phát triển, ứng dụng sản phẩm mật mã dân sự để bảo mật thông tin.

b) Xây dựng kiến trúc bảo vệ an ninh mạng quốc gia đồng bộ, thống nhất, đa lớp hỗ trợ bảo vệ cho toàn bộ hạ tầng mạng Internet Việt Nam và hệ thống thông tin của bộ, cơ quan, địa phương, tổ chức, doanh nghiệp. Trong đó, tập trung xây dựng và vận hành hiệu quả Hệ thống phòng vệ mạng quốc gia, Nền tảng điều hành an ninh mạng quốc gia và các nền tảng số dùng chung quốc gia chuyên ngành an ninh mạng là nền tảng dùng chung trong Khung kiến trúc tổng thể quốc gia số nhằm bảo vệ an ninh mạng 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; có khả năng tích hợp, kết nối với các sản phẩm an ninh mạng phù hợp, đáp ứng tiêu chuẩn, quy chuẩn về an ninh mạng. Nâng cao năng lực của Trung tâm An ninh mạng quốc gia thuộc Bộ Công an. Hướng dẫn xây dựng trung tâm an ninh mạng tại các tỉnh, thành phố. Ban hành danh mục thiết bị tối thiểu cần có tại các trung tâm an ninh mạng. Mở rộng kết nối giám sát an ninh mạng đến toàn bộ cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành, hệ thống thông tin, hệ thống dùng chung của toàn hệ thống chính trị. Đôn đốc các cơ quan, ban, bộ, ngành, địa phương thiết lập kênh kết nối trao đổi thông tin, dữ liệu phục vụ giám sát, điều phối ứng cứu, khắc phục sự cố an ninh mạng theo hướng dẫn của lực lượng chuyên trách.

c) Xây dựng, hoàn thiện hệ thống tiêu chuẩn, quy chuẩn kỹ thuật quốc gia về an ninh mạng; tổ chức rà soát, kiểm tra, đánh giá định kỳ công tác bảo đảm an ninh thông tin, an ninh mạng. Tập trung phát triển giải pháp kỹ thuật bảo đảm tuyệt đối an toàn cho các hệ thống thông tin trọng yếu; tăng cường phối hợp chặt chẽ, hiệp đồng tác chiến giữa các lực lượng chuyên trách trong bảo vệ an ninh mạng toàn hệ thống chính trị.

d) Rà soát, điều chỉnh quy hoạch hạ tầng công nghệ thông tin theo hướng tập trung máy chủ về các trung tâm dữ liệu đạt chuẩn, đủ điều kiện an ninh mạng. Tăng cường bảo đảm an ninh kết nối, duy trì sự ổn định, thông suốt và an toàn của các luồng dữ liệu quốc gia, kết nối quốc tế trong mọi tình huống, kể cả khi xảy ra thảm họa, chiến tranh.

đ) Bảo đảm nguồn lực tài chính bền vững cho công tác an ninh mạng. Thực hiện nghiêm quy định ưu tiên sử dụng sản phẩm, giải pháp an ninh mạng trong nước trong các dự án đầu tư công. Bảo đảm tỉ lệ kinh phí chi cho an ninh mạng, bảo mật thông tin đạt tối thiểu 15% tổng kinh phí triển khai kế hoạch ứng dụng công nghệ thông tin, chuyển đổi số; đầu tư có trọng tâm, trọng điểm, tránh dàn trải, lãng phí.

4. Xây dựng thế trận an ninh nhân dân gắn với thế trận quốc phòng toàn dân trên không gian mạng; phát triển tiềm lực, công nghệ và nguồn nhân lực

a) Xây dựng thế trận an ninh nhân dân gắn với thế trận quốc phòng toàn dân trên không gian mạng vững chắc. Phát huy vai trò nòng cốt của lực lượng vũ trang nhân dân; huy động sức mạnh tổng hợp của các doanh nghiệp công nghệ, viễn thông và các tầng lớp nhân dân. Các doanh nghiệp cung cấp dịch vụ viễn thông, Internet phải xác định rõ trách nhiệm là "tuyến đầu" trong bảo vệ an ninh mạng.

b) Tập trung nguồn lực xây dựng nền công nghiệp an ninh mạng tự chủ, tự cường; ưu tiên phát triển các sản phẩm "Make in Vietnam". Trong đó, chú trọng làm chủ và sản xuất các sản phẩm cốt lõi, nền tảng bao gồm: Giải pháp tường lửa, phòng, chống mã độc, bảo vệ thiết bị đầu cuối, nền tảng điện toán đám mây và hệ điều hành dùng riêng. Xây dựng cơ chế, chính sách hỗ trợ, thu hút doanh nghiệp công nghệ, cộng đồng khởi nghiệp sáng tạo tham gia phát triển hệ sinh thái an ninh mạng. Tăng cường công tác đánh giá, kiểm định, chứng nhận hợp chuẩn, hợp quy; tạo điều kiện thuận lợi cho doanh nghiệp thương mại hoá sản phẩm, dịch vụ, hướng tới xuất khẩu và cạnh tranh quốc tế.

c) Đẩy mạnh đào tạo, phát triển nguồn nhân lực an ninh mạng chất lượng cao. Tăng cường liên kết giữa Nhà nước - Nhà trường - Doanh nghiệp trong đào tạo, huấn luyện thực chiến. Xây dựng mạng lưới chuyên gia an ninh mạng trong và ngoài nước, sẵn sàng huy động nguồn lực xã hội tham gia ứng cứu sự cố, tình huống nguy hiểm về an ninh mạng. Tiếp tục hoàn thiện cơ chế, chính sách thu hút, đãi ngộ chuyên gia giỏi, nhân tài tham gia phục vụ công tác an ninh mạng quốc gia.

5. Về hợp tác quốc tế trên lĩnh vực an ninh mạng

a) Tăng cường và làm sâu sắc hơn quan hệ hợp tác song phương, đa phương trên lĩnh vực an ninh mạng, trọng tâm là chia sẻ thông tin tình báo, cảnh báo sớm; phối hợp quốc tế phòng, chống và ứng phó sự cố tấn công mạng; điều tra, truy tố tội phạm mạng xuyên quốc gia; bảo đảm độc lập, tự chủ, chủ quyền quốc gia trong quá trình hợp tác, tiếp thu kinh nghiệm, công nghệ và chuẩn mực quốc tế về an ninh mạng.

b) Triển khai hiệu quả, thực chất Công ước của Liên hợp quốc về chống tội phạm mạng năm 2025 (Công ước Hà Nội). Chủ động tham gia xây dựng các khuôn khổ pháp lý, chuẩn mực chung của quốc tế; sớm nghiên cứu, ban hành Tuyên bố quốc gia của Việt Nam về việc áp dụng luật pháp quốc tế trên không gian mạng để khẳng định chủ quyền và trách nhiệm quốc gia. Tăng cường

phối hợp, chia sẻ thông tin với lực lượng chức năng các nước; cử cán bộ đi đào tạo, huấn luyện chuyên sâu tại nước ngoài và tích cực tham gia các cuộc diễn tập an ninh mạng quốc tế. Nghiên cứu, đề xuất thành lập Trung tâm đào tạo khu vực về phòng, chống tội phạm mạng và an ninh mạng tại Việt Nam để nâng cao vị thế và năng lực dẫn dắt trong khu vực.

6. Tổ chức thực hiện

a) Các tỉnh uỷ, thành uỷ, các ban đảng Trung ương: Tổ chức quán triệt, xây dựng chương trình hành động thực hiện Chỉ thị; chịu trách nhiệm trước Ban Bí thư về kết quả công tác bảo đảm an ninh mạng tại địa phương, cơ quan, đơn vị mình.

b) Đảng uỷ Quốc hội, Đảng uỷ Chính phủ:

- Lãnh đạo, chỉ đạo xây dựng chương trình hành động và tổ chức triển khai thực hiện Chỉ thị.

- Lãnh đạo, chỉ đạo rà soát, sửa đổi, bổ sung hệ thống pháp luật về an ninh mạng, cơ yếu, bảo vệ bí mật nhà nước và các văn bản liên quan để thể chế hoá kịp thời các quan điểm, nhiệm vụ, giải pháp nêu tại Chỉ thị này.

- Chỉ đạo các cơ quan liên quan đề xuất xây dựng, ban hành cơ chế, chính sách đột phá đặc thù, ưu đãi vượt trội để thu hút, giữ chân các chuyên gia, nhân tài an ninh mạng, đào tạo nhân lực chất lượng cao, hướng tới mục tiêu cả nước có 10.000 chuyên gia an ninh mạng vào năm 2030.

c) Đảng uỷ Công an Trung ương: Lãnh đạo, chỉ đạo Bộ Công an:

- 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, cơ yếu); quản lý nhà nước về sản phẩm mật mã an ninh.

- Chủ trì xây dựng, công bố Bộ chỉ số bảo đảm an ninh mạng quốc gia và tổ chức đánh giá, xếp hạng định kỳ hằng năm đối với các ban, bộ, ngành, địa phương.

- Nghiên cứu, xây dựng, phát triển và ứng dụng sản phẩm mật mã dân sự vào công tác bảo đảm an ninh mạng quốc gia theo quy định; chủ trì triển khai các nhiệm vụ về phát triển và ứng dụng sản phẩm mật mã an ninh; chỉ đạo huy động các nguồn lực xã hội tham gia bảo vệ an ninh mạng quốc gia.

- Chủ trì, phối hợp đẩy mạnh kết nối, sử dụng dữ liệu từ cơ sở dữ liệu quốc gia về dân cư để thống nhất định danh không gian mạng toàn diện; tập trung chỉ đạo xử lý dứt điểm tình trạng SIM "rác", tài khoản "ảo" và thiết lập trật tự, kỷ cương trong quản lý người dùng mạng xã hội; bảo đảm các yêu cầu về bảo vệ an ninh mạng quốc gia, bảo vệ dữ liệu cá nhân và bảo vệ trẻ em trên không gian mạng.

d) 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, cơ yếu thuộc phạm vi quản lý của Bộ Quốc phòng.

- Đảng uỷ Ban Cơ yếu Chính phủ lãnh đạo thống nhất quản lý nhà nước về mật mã (bao gồm mật mã cơ yếu, mật mã dân sự) và sản phẩm mật mã cơ yếu. Phối hợp chặt chẽ với Đảng uỷ Công an Trung ương trong công tác bảo đảm an ninh mạng chung.

đ) Đảng uỷ Bộ Giáo dục và Đào tạo: Chủ trì, phối hợp xây dựng chương trình, tổ chức đào tạo nguồn nhân lực an ninh mạng chất lượng cao; tích hợp kiến thức an ninh mạng vào hệ thống giáo dục quốc dân.

e) Ban Tuyên giáo và Dân vận Trung ương: Chủ trì chỉ đạo, định hướng công tác tuyên truyền, phổ biến, quán triệt Chỉ thị sâu rộng trong toàn Đảng và toàn xã hội.

g) Văn phòng Trung ương Đảng: Chủ trì, phối hợp với Đảng uỷ Công an Trung ương và Quân uỷ Trung ương theo dõi, đôn đốc, kiểm tra và định kỳ báo cáo Ban Bí thư việc thực hiện Chỉ thị.

Chỉ thị này phổ biến đến chi bộ.

T/M BAN BÍ THƯ

ĐẢNG CỘNG SẢN VIỆT NAM
BAN CHẤP HÀNH TRUNG ƯƠNG

Trần Cẩm Tú

Nơi nhận:
- Bộ Chính trị, Ban Bí thư (để báo cáo),
- Các cơ quan, ban đảng Trung ương,
- Các tỉnh uỷ, thành uỷ, đảng uỷ trực thuộc Trung ương,
- Đảng uỷ các bộ, ngành, tổ chức chính trị - xã hội ở Trung ương,
- Các đảng uỷ đơn vị sự nghiệp Trung ương,
- Các đồng chí Uỷ viên Ban Chấp hành Trung ương Đảng,
- Lưu Văn phòng Trung ương Đảng.

TỈNH ỦY HƯNG YÊN
VĂN PHÒNG
*
Số 84 - BS/VPTU

Nơi nhận:
- Các ban đảng tỉnh, ĐUTTTU,
- Đảng ủy UBND tỉnh,
- Sở Khoa học công nghệ tỉnh,
- Các đơn vị sự nghiệp thuộc Tỉnh ủy,
- Các đ/c UVBTVTU,
- Lưu VPTU.

SAO Y

Hưng Yên, ngày 29 tháng 01 năm 2026

K/T CHÁNH VĂN PHÒNG
PHÓ CHÁNH VĂN PHÒNG

ĐẢNG CỘNG SẢN VIỆT NAM
VĂN PHÒNG
TỈNH ỦY HƯNG YÊN

Thái Văn Minh