

KẾ HOẠCH

Thực hiện 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

Thực hiện Chương trình hành động số 09-CTr/TU ngày 13/02/2026 của Ban Thường vụ Tỉnh ủy về việc thực hiện 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 (sau đây viết gọn là *Chỉ thị số 57-CT/TW*); Sở Tài chính ban hành Kế hoạch triển khai thực hiện, như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Quán triệt, triển khai thực hiện Chỉ thị số 57-CT/TW, tạo sự thống nhất cao trong nhận thức và hành động của cán bộ, đảng viên, công chức, viên chức và người lao động, coi đây là nhiệm vụ trọng tâm, thường xuyên trong công tác bảo đảm an ninh quốc gia, giữ gìn trật tự an toàn xã hội, góp phần quản lý hiệu quả, an toàn phục vụ phát triển kinh tế - xã hội của địa phương.

2. Cụ thể hóa và tổ chức thực hiện có hiệu quả các quan điểm, mục tiêu, nhiệm vụ nêu tại Chỉ thị số 57-CT/TW gắn với thực hiện Nghị quyết Đại hội Đảng bộ tỉnh Hưng Yên lần thứ I, nhiệm kỳ 2025 - 2030 và Nghị quyết Đại hội Đảng toàn quốc lần thứ XIV. Tăng cường sự lãnh đạo của các cấp ủy, tổ chức đảng, nâng cao nhận thức, trách nhiệm của cả hệ thống chính trị và toàn thể cán bộ, đảng viên, công chức, viên chức và người lao động về an ninh mạng, bảo mật thông tin, an ninh dữ liệu; chủ động sẵn sàng ứng phó với các nguy cơ, thách thức từ không gian mạng.

3. Đề ra các nhiệm vụ cần triển khai thực hiện trong thời gian tới, xác định rõ các công việc, phân công trách nhiệm thực hiện cụ thể; kịp thời đề xuất các giải pháp tháo gỡ khó khăn, vướng mắc phát sinh trong quá trình thực hiện.

II. MỤC TIÊU

1. **Về trung tâm an ninh mạng:** 100% hệ thống thông tin của Sở được bảo vệ theo mô hình 4 lớp và được giám sát an toàn thông tin 24/7.

2. **Về hạ tầng dữ liệu:** 100% dữ liệu dùng chung, dữ liệu chuyên ngành được lưu trữ tập trung tại Trung tâm dữ liệu tỉnh đạt chuẩn an ninh mạng; chấm dứt tình trạng máy chủ phân tán, không bảo đảm an toàn tại các đơn vị.

3. **Về nguồn lực tài chính:** Trên cơ sở đề xuất của các phòng, đơn vị, căn cứ tiêu chuẩn định mức, chi ngân sách hiện hành, Văn phòng Sở báo cáo Lãnh đạo Sở tham mưu UBND tỉnh bố trí nguồn kinh phí ngân sách nhà nước theo phân cấp cho công tác an ninh mạng và các dự án an ninh mạng theo quy định của Luật ngân sách nhà nước, Luật Đầu tư công và các văn bản pháp luật có liên quan.

4. Về nguồn nhân lực: Xây dựng đội ngũ của Sở đủ năng lực làm chủ công nghệ; 100% cán bộ chuyên trách công nghệ thông tin tại sở được đào tạo, bồi dưỡng chuyên sâu về an ninh mạng.

5. Về nhận thức xã hội: Triển khai sâu rộng phong trào “Bình dân học vụ số”; phấn đấu 100% cán bộ, đảng viên, công chức, viên chức và người lao động sử dụng thiết bị thông minh được trang bị kỹ năng cơ bản về an toàn thông tin, nhận diện và phòng chống lừa đảo trực tuyến.

III. NHIỆM VỤ, GIẢI PHÁP

1. Tăng cường sự lãnh đạo của Đảng, nâng cao nhận thức, trách nhiệm của cả hệ thống chính trị và toàn thể cán bộ, đảng viên, công chức, viên chức và người lao động về an ninh mạng, bảo mật thông tin, an ninh dữ liệu

- Tăng cường sự lãnh đạo, chỉ đạo của các cấp ủy đảng, đẩy mạnh công tác tuyên truyền, thống nhất nhận thức về 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 cán bộ, đảng viên, công chức, viên chức, người lao động.

- Các cấp ủy, tổ chức đảng, cán bộ, đảng viên cần đổi mới tư duy, nâng cao nhận thức, gắn trách nhiệm người đứng đầu trong triển khai thực hiện nhiệm vụ, phải trực tiếp phụ trách, chỉ đạo rà soát, xác định rõ những vấn đề trọng tâm, trọng điểm để chỉ đạo; cán bộ, đảng viên phải gương mẫu thực hiện nghiêm túc, hiệu quả công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu.

- 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.

- 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 là 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.

- 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.

- Người đứng đầu cấp ủy, chính quyền, cơ quan, phòng, 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 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.

- Đổi mới mạnh mẽ nội dung, hình thức tuyên truyền, giáo dục kiến thức, kỹ năng an ninh mạng. 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.

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

Thực hiện nghiêm quy định pháp luật yêu cầu hồ sơ thiết kế hệ thống thông tin, các dự án chuyên đổi số trên địa bàn tỉnh phải có cầu phần an ninh mạng được thẩm định, phê duyệt trước khi đầu tư xây dựng.

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

- Nâng cao trách nhiệm tự bảo vệ hệ thống thông tin thuộc phạm vi quản lý. Gắn trách nhiệm của người đứng đầu cơ quan chủ quản hệ thống thông tin với trách nhiệm bảo đảm an toàn, an ninh mạng. Xây dựng, cập nhật, vận hành hệ thống thông tin theo tiêu chuẩn, quy chuẩn kỹ thuật về an toàn, an ninh. Rà soát, lập hồ sơ đề nghị đưa các hệ thống thông tin trọng yếu, phù hợp với quy định của pháp luật vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia (nếu có).

- Thực hiện nghiêm túc các quy định pháp luật về bảo vệ an ninh mạng; xác định cấp độ và trách nhiệm bảo đảm an toàn hệ thống thông tin theo từng cấp độ và triển khai mô hình bảo vệ 4 lớp trước khi đưa vào sử dụng. Chủ động giám sát, kịp thời phát hiện nguy cơ mất an toàn, an ninh mạng trong quá trình thi công, lắp đặt thiết bị trong các hệ thống thông tin. Ưu tiên sử dụng sản phẩm, giải pháp an toàn, an ninh mạng “Make in Viet Nam”.

- Đầu tư nguồn lực, thường xuyên nâng cấp hệ thống, cập nhật bản quyền, nâng cao nhận thức và kỹ năng an toàn, an ninh mạng cho cán bộ, đảng viên, công chức, viên chức và người lao động. Sử dụng các giải pháp dùng mật mã để bảo vệ thông tin trong hệ thống thông tin của cơ quan theo quy định.

- 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 bảo đảm an ninh kết nối, duy trì sự ổn định, thông suốt và an toàn của các luồng dữ liệu, kết nối trong mọi tình huống, không để xảy ra bị động, bất ngờ.

- 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. Bảo đảm tỷ 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.

IV. TỔ CHỨC THỰC HIỆN

1. Các phòng, đơn vị căn cứ chức năng, nhiệm vụ được giao, tổ chức nghiên cứu, quán triệt, tuyên truyền và triển khai thực hiện Chỉ thị số 57-CT/TW theo Chương trình hành động của Ban Thường vụ Tỉnh ủy; chịu trách nhiệm trước Lãnh đạo Sở về kết quả công tác bảo đảm an ninh mạng tại cơ quan.

2. Văn phòng Sở và các phòng, đơn vị liên quan theo dõi, kiểm tra, giám sát, đánh giá kết quả thực hiện, định kỳ báo cáo theo quy định

3. Quá trình tổ chức triển khai thực hiện, Văn phòng Sở tham mưu Lãnh đạo Sở quyết định việc điều chỉnh, bổ sung các nhiệm vụ cụ thể trong Kế hoạch này để phù hợp với điều kiện tình hình thực tiễn, đáp ứng các yêu cầu nhiệm vụ chính trị của cơ quan./

Nơi nhận:

- Các đ/c Lãnh đạo Sở;
- Các phòng, đơn vị thuộc Sở;
- Lưu VT, VPS.

GIÁM ĐỐC



Nguyễn Đức Tài

Ký bởi: SỞ TÀI CHÍNH
Cấp ủy viên AN NINH DÂN
TỈNH HƯNG YÊN
Thời gian ký: 24/02/2026 15:51:46