TỈNH ỦY BẮC NINH
TIỂU BAN AN NINH MẠNG
*
Số 11 -KH/TBANM

ĐẢNG CỘNG SẢN VIỆT NAM

Bắc Ninh, ngày 19 tháng 5 năm 2026

KẾ HOẠCH
ứng phó sự cố, bảo đảm an ninh mạng trên địa bàn tỉnh Bắc Ninh

---

Căn cứ Chương trình hành động số 17-CTr/TU ngày 27/02/2026 của Ban Thường vụ Tỉnh ủy Bắc Ninh về 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 *(gọi tắt là "Chương trình hành động số 17")*; Kế hoạch số 132/KH-UBND tỉnh ngày 22/4/2026 của Chủ tịch UBND tỉnh về triển khai Chương trình hành động số 17; Quyết định số 03-QĐ/TBANM ngày 22/4/2026 của Trưởng Tiểu ban An ninh mạng tỉnh về thành lập Đội ứng cứu sự cố an ninh mạng tỉnh Bắc Ninh (gọi tắt là "Đội ứng cứu sự cố"); Quyết định số 04-QĐ/TBANM ngày 22/4/2026 của Trưởng Tiểu ban An ninh mạng tỉnh về ban hành Quy chế hoạt động của Đội ứng cứu sự cố; Tiểu ban An ninh mạng tỉnh (TBANM) ban hành Kế hoạch ứng phó sự cố, bảo đảm an ninh mạng trên địa bàn tỉnh Bắc Ninh như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Bảo đảm an ninh mạng cho các hệ thống thông tin trên địa bàn tỉnh; bảo đảm khả năng thích ứng một cách chủ động, linh hoạt và giảm thiểu các nguy cơ, mối đe dọa an ninh mạng, kịp thời khắc phục các tồn tại, lỗ hổng, điểm yếu nhằm phòng ngừa các sự cố tấn công mạng; đề ra các giải pháp ứng phó khi gặp sự cố an ninh mạng.

- Tạo chuyển biến mạnh mẽ trong nhận thức về an ninh mạng đối với cán bộ, công chức, viên chức trong các cơ quan nhà nước của tỉnh.

- Xây dựng, phát triển Đội ứng cứu sự cố có đầy đủ kiến thức, kỹ năng xử lý sự cố an ninh mạng đảm bảo linh hoạt, hiệu quả, phù hợp với yêu cầu thực tế.

- Đảm bảo các nguồn lực và các điều kiện cần thiết để sẵn sàng triển khai kịp thời, hiệu quả các phương án ứng cứu khẩn cấp sự cố an ninh mạng.

2. Yêu cầu

- Các hệ thống thông tin của các cơ quan, đơn vị, địa phương phải được đánh giá hiện trạng và khả năng bảo đảm an ninh mạng, dự báo các nguy cơ, sự cố, tấn công mạng có thể xảy ra để đưa ra phương án ứng phó, ứng cứu sự cố kịp thời, phù hợp.

- Hoạt động ứng cứu sự cố an ninh mạng phải chuyển từ bị động sang chủ động, bao gồm: Chủ động thực hiện săn lùng mối nguy hại và rà quét lỗ hổng trên các hệ thống thông tin trong phạm vi quản lý.

- Xác định cụ thể các nguồn lực, giải pháp tổ chức thực hiện và kinh phí để triển khai các nội dung của Kế hoạch, bảo đảm khả thi, hiệu quả.

- Thường xuyên trao đổi thông tin, chia sẻ kinh nghiệm trong công tác bảo đảm an ninh mạng giữa các cơ quan nhà nước trên địa bàn tỉnh; tận dụng sự phối hợp, hỗ trợ của cơ quan điều phối quốc gia về ứng cứu sự cố (Trung tâm An ninh mạng quốc gia - Bộ Công an).

- Thực hiện đúng các quy định của pháp luật về quy trình xử lý sự cố an ninh mạng; chủ động phát hiện, báo cáo, phối hợp xử lý kịp thời các nguy cơ, hành vi tấn công mạng, rò rỉ dữ liệu hoặc xâm phạm hệ thống thông tin.

II. CÁC QUY ĐỊNH CHUNG

1. Phạm vi và đối tượng

Kế hoạch này để ứng phó sự cố an ninh mạng đối với các hệ thống thông tin trên địa bàn tỉnh; áp dụng cho các cơ quan, đơn vị làm chủ quản, quản lý, vận hành, sử dụng các hệ thống thông tin trên địa bàn tỉnh, các doanh nghiệp có liên quan, Đội ứng cứu sự cố.

2. Nguyên tắc, phương châm ứng phó sự cố

- Tuân thủ các quy định pháp luật về điều phối, ứng cứu sự cố an ninh mạng.

- Khảo sát, đánh giá đầy đủ các nguy cơ, sự cố an ninh mạng của hệ thống thông tin để đưa ra các phương án đối phó, ứng cứu sự cố tương ứng, kịp thời, phù hợp theo tình hình thực tế.

- Phương án đối phó, ứng cứu sự cố an ninh mạng phải đặt ra được các tiêu chí để có thể nhanh chóng xác định được tính chất, mức độ nghiêm trọng khi sự cố xảy ra.

- Ứng cứu sự cố trước hết phải được thực hiện, xử lý bằng lực lượng tại chỗ và trách nhiệm chính của chủ quản hệ thống thông tin.

- Thông tin trao đổi trong mạng lưới phải được kiểm tra, xác thực đối tượng trước khi thực hiện các bước tác nghiệp tiếp theo.

- Bảo đảm bí mật thông tin khi tham gia, thực hiện các hoạt động ứng cứu sự cố theo yêu cầu của cơ quan điều phối quốc gia hoặc cơ quan, tổ chức, cá nhân gặp sự cố.

- Ưu tiên bố trí nguồn lực; triển khai đồng bộ giải pháp tổ chức thực hiện nhằm bảo đảm các nội dung của kế hoạch khả thi, hiệu quả cao.

3. Các lực lượng tham gia ứng phó sự cố

- Chủ quản hệ thống thông tin, Đội ứng cứu sự cố, Trung tâm an ninh mạng

quốc gia - Bộ Công an.

- Công an tỉnh; Bộ chỉ huy quân sự tỉnh; các sở, ban, ngành, đoàn thể của tỉnh; Đảng ủy, UBND các xã, phường; các cơ quan, đơn vị, doanh nghiệp có liên quan.

- Đơn vị quản lý, vận hành hệ thống thông tin.

- Doanh nghiệp cung cấp dịch vụ an ninh mạng (trường hợp thuê dịch vụ).

4. Chức năng, nhiệm vụ, trách nhiệm và cơ chế, quy trình phối hợp giữa các cơ quan, đơn vị

- Công an tỉnh: Đơn vị chuyên trách ứng cứu sự cố an ninh mạng của tỉnh; thực hiện chỉ đạo, tổ chức triển khai hoạt động ứng phó sự cố an ninh mạng và các nhiệm vụ khác khi xảy ra sự cố.

- Đội ứng cứu sự cố: Do chủ quản hệ thống thông tin của tỉnh thành lập, là lực lượng chính tham gia các hoạt động ứng cứu sự cố an ninh mạng; thực hiện nhiệm vụ theo Quy chế hoạt động của Đội; tham gia hoạt động ứng cứu khẩn cấp bảo đảm an ninh mạng quốc gia khi có yêu cầu từ Bộ Công an hoặc các bộ, ngành có liên quan.

- Sở Khoa học và Công nghệ: Chịu trách nhiệm xây dựng, thực thi các quy định về an toàn bảo mật thông tin mạng, quản lý, khai thác và vận hành Trung tâm tích hợp dữ liệu; cử thành viên tham gia Đội ứng cứu sự cố, xử lý, ứng cứu các sự cố an ninh mạng, an ninh mạng xảy ra trên địa bàn tỉnh khi có yêu cầu của đơn vị điều phối.

- Các cơ quan, đơn vị: Có trách nhiệm cử cán bộ, công chức, viên chức phụ trách an ninh mạng tham gia Đội ứng cứu sự cố khi xử lý sự cố. Phối hợp với đơn vị chuyên trách ứng cứu sự cố an ninh mạng của tỉnh trong công tác ứng phó, xử lý các sự cố.

- Doanh nghiệp cung cấp, xây dựng các hệ thống thông tin: Phối hợp với Công an tỉnh, chủ quản hệ thống thông tin, đơn vị quản lý, vận hành hệ thống thông tin trong công tác ứng phó, xử lý các sự cố an ninh mạng liên quan hệ thống thông tin do mình xây dựng hoặc cung cấp.

- Doanh nghiệp cung cấp dịch vụ viễn thông internet: Phối hợp với Công an tỉnh, chủ quản hệ thống thông tin, đơn vị quản lý, vận hành hệ thống thông tin trong công tác ứng phó, xử lý các sự cố an ninh mạng liên quan đến hạ tầng viễn thông, dịch vụ Internet do mình cung cấp hoặc quản lý.

III. NỘI DUNG THỰC HIỆN

1. Đánh giá các nguy cơ, sự cố an ninh mạng

a) Nội dung thực hiện: Đánh giá hiện trạng, khả năng bảo đảm an ninh mạng, dự báo các nguy cơ, sự cố, tấn công mạng có thể xảy ra với các hệ thống thông tin và các đối tượng cần bảo vệ; đánh giá, dự báo các hậu quả, thiệt hại, tác động nếu

xảy ra sự cố; đánh giá về hiện trạng phương tiện, trang thiết bị, công cụ hỗ trợ nhân lực, vật lực phục vụ đối phó, ứng cứu, khắc phục sự cố (bao gồm cả đơn vị cung cấp dịch vụ nếu có).

- Đơn vị chủ trì: Cơ quan, đơn vị quản lý, vận hành hệ thống thông tin.

- Đơn vị phối hợp: Công an tỉnh; Đội ứng cứu sự cố; Sở Khoa học và Công nghệ; các doanh nghiệp cung cấp dịch vụ viễn thông, internet; doanh nghiệp cung cấp dịch vụ an ninh mạng (trường hợp thuê dịch vụ) và các cơ quan, đơn vị khác có liên quan.

- Thời gian thực hiện: Thường xuyên.

b) Nội dung thực hiện: Chủ động thực hiện săn lùng mối nguy hại và rà quét lỗ hổng trên các hệ thống thông tin trong phạm vi quản lý; khắc phục các lỗ hổng, điểm yếu theo cảnh báo của cơ quan chức năng[1].

- Đơn vị chủ trì: Đơn vị quản lý, vận hành hệ thống thông tin.

- Đơn vị phối hợp: Công an tỉnh; Đội ứng cứu sự cố; Sở Khoa học và Công nghệ; các doanh nghiệp cung cấp dịch vụ viễn thông, internet; doanh nghiệp cung cấp dịch vụ an ninh mạng (trường hợp thuê dịch vụ) và các cơ quan, đơn vị khác có liên quan.

- Thời gian thực hiện: hằng năm (tối thiểu 01 lần/06 tháng).

2. Phương án ứng cứu đối với một số tình huống sự cố cụ thể

Đối với mỗi hệ thống thông tin, chương trình ứng dụng, cần xây dựng tình huống, kịch bản sự cố cụ thể và đưa ra phương án đối phó, ứng cứu sự cố tương ứng. Trong phương án đối phó, ứng cứu phải đặt ra được các tiêu chí để có thể nhanh chóng xác định được tính chất, mức độ của sự cố khi sự cố xảy ra. Việc xây dựng phương án đối phó, ứng cứu sự cố và tuân thủ theo các quy định, hướng dẫn, đảm bảo các nội dung sau:

a) Quy trình triển khai và các bước ưu tiên ứng cứu ban đầu khi hệ thống thông tin gặp sự cố, có phân theo các loại sự cố thực hiện theo mục 3, Phần III. Triển khai hoạt động thường trực, điều phối, xử lý, ứng cứu sự cố của Kế hoạch này.

b) Phương pháp, cách thức để xác định nhanh chóng, kịp thời nguyên nhân, nguồn gốc sự cố nhằm áp dụng phương án đối phó, ứng cứu, khắc phục sự cố phù hợp. Các sự cố thường gặp:

- Sự cố do bị tấn công mạng.

- Sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật hoặc do lỗi đường điện, đường truyền, hosting...

- Sự cố do lỗi của người quản trị, vận hành hệ thống.

---

[1] Thực hiện theo quy định tại 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 tại Việt Nam.

- Sự cố liên quan đến các thiên tai, thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn và các sự cố an ninh mạng khác.

c) Phương án đối phó, khắc phục sự cố đối với một hoặc nhiều tình huống.

- Tình huống sự cố do bị tấn công mạng:

+ Tấn công từ chối dịch vụ;

+ Tấn công giả mạo;

+ Tấn công sử dụng mã độc;

+ Tấn công truy cập trái phép, chiếm quyền điều khiển;

+ Tấn công thay đổi giao diện;

+ Tấn công mã hóa phần mềm, dữ liệu, thiết bị;

+ Tấn công phá hoại thông tin, dữ liệu, phần mềm;

+ Tấn công nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu;

+ Tấn công tổng hợp sử dụng kết hợp nhiều hình thức;

+ Các hình thức tấn công mạng khác.

- Tình huống sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật:

+ Sự cố nguồn điện;

+ Sự cố đường kết nối Internet;

+ Sự cố do lỗi phần mềm, phần cứng, ứng dụng của hệ thống thông tin;

+ Sự cố liên quan đến quá tải hệ thống;

+ Sự cố khác do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật.

- Tình huống sự cố do lỗi của người quản trị, vận hành hệ thống:

+ Lỗi trong cập nhật, thay đổi, cấu hình phần cứng;

+ Lỗi trong cập nhật, thay đổi, cấu hình phần mềm;

+ Lỗi liên quan đến chính sách và thủ tục an ninh mạng;

+ Lỗi liên quan đến việc dừng dịch vụ vì lý do bắt buộc;

+ Lỗi khác liên quan đến người quản trị, vận hành hệ thống.

- Tình huống sự cố liên quan đến các thiên tai, thảm họa tự nhiên, như bão, lụt, động đất, hỏa hoạn và các sự cố an ninh mạng khác.

d) Công tác tổ chức, điều hành, phối hợp giữa các lực lượng, các tổ chức trong đối phó, ngăn chặn, ứng cứu, khắc phục sự cố.

- Đơn vị chủ trì: Công an tỉnh.

- Đơn vị phối hợp: Cơ quan điều phối quốc gia Trung tâm An ninh mạng quốc gia; các sở, ban, ngành, đoàn thể của tỉnh; UBND các xã, phường; Đội ứng cứu sự cố; Sở Khoa học và Công nghệ; các doanh nghiệp cung cấp dịch vụ viễn thông, internet; doanh nghiệp cung cấp dịch vụ an ninh mạng (nếu có); các cơ quan, đơn vị khác có liên quan.

- Thời gian thực hiện: Thường xuyên hằng năm.

đ) Phương án về nhân lực, trang thiết bị, phần mềm, phương tiện, công cụ và dự kiến kinh phí để thực hiện, đối phó, ứng cứu, xử lý đối với từng tình huống sự cố cụ thể.

- Đơn vị chủ trì: Các sở, ban, ngành, đoàn thể của tỉnh; UBND các xã, phường.

- Đơn vị phối hợp: Công an tỉnh; Đội ứng cứu sự cố; Sở Khoa học và Công nghệ; các doanh nghiệp cung cấp dịch vụ viễn thông, internet; doanh nghiệp cung cấp dịch vụ an ninh mạng (nếu có); các cơ quan, đơn vị khác có liên quan.

- Thời gian thực hiện: Thường xuyên hằng năm.

3. Triển khai hoạt động thường trực, điều phối, xử lý, ứng cứu sự cố

a) Thông báo, báo cáo sự cố an ninh mạng

- Đơn vị thực hiện: Đơn vị quản lý, vận hành hệ thống thông tin báo cáo cơ quan Chủ quản hệ thống thông tin, Công an tỉnh, Đội ứng cứu sự cố, đồng gửi Cơ quan điều phối quốc gia (Trung tâm An ninh mạng quốc gia).

- Thời gian thực hiện: Ngay khi xảy ra sự cố và được duy trì trong suốt quá trình ứng cứu sự cố.

b) Phát hiện, tiếp nhận, xác minh, xử lý ban đầu sự cố an ninh mạng

- Đơn vị chủ trì: Công an tỉnh; cơ quan, đơn vị quản lý, vận hành hệ thống thông tin; Đội ứng cứu sự cố.

- Đơn vị phối hợp: Cơ quan điều phối quốc gia (Trung tâm An ninh mạng quốc gia); Sở Khoa học và Công nghệ; tổ chức, cá nhân gửi thông báo, báo cáo sự cố; các doanh nghiệp cung cấp dịch vụ viễn thông, internet; doanh nghiệp cung cấp dịch vụ an ninh mạng (nếu có); các cơ quan, đơn vị chức năng liên quan.

- Thời gian thực hiện: Ngay sau khi phát hiện sự cố hoặc nhận được thông báo, báo cáo sự cố của tổ chức, cá nhân.

c) Quy trình ứng cứu sự cố an ninh mạng thông thường và nghiêm trọng theo quy định tại Điều 13 và Điều 14 Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ về ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia và Điều 11 Thông tư 20/2017/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc *(Sơ đồ tại phụ lục kèm theo kế hoạch).*

- Đơn vị chủ trì: Công an tỉnh.

- Đơn vị phối hợp: Cơ quan, đơn vị quản lý, vận hành hệ thống thông tin; Đội ứng cứu sự cố; Sở Khoa học và Công nghệ.

- Thời gian thực hiện: Hằng năm.

4. Triển khai huấn luyện, diễn tập, phòng ngừa sự cố, giám sát phát hiện, bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố

Xây dựng các nội dung, nhiệm vụ cụ thể cần triển khai nhằm phòng ngừa sự

cố, giám sát phát hiện, huấn luyện, diễn tập, bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố. Đồng thời cần đáp ứng đúng theo quy định tại Chỉ thị số 60/CT-BTTTT ngày 16/9/2021 của Bộ trưởng Bộ Thông tin và Truyền thông về việc tổ chức triển khai diễn tập thực chiến bảo đảm an ninh mạng, bao gồm:

a) Triển khai các chương trình huấn luyện, diễn tập.

- Nội dung thực hiện: Tổ chức diễn tập các phương án đối phó, ứng cứu sự cố tương ứng với các kịch bản, tình huống sự cố cụ thể; huấn luyện, diễn tập nâng cao kỹ năng, nghiệp vụ phối hợp, ứng cứu, chống tấn công, xử lý mã độc, khắc phục sự cố; tham gia huấn luyện, diễn tập vùng, miền, quốc gia, quốc tế.

- Đơn vị chủ trì: Công an tỉnh; Đội ứng cứu sự cố.

- Đơn vị phối hợp: Đơn vị quản lý, vận hành hệ thống thông tin; Cơ quan điều phối quốc gia (Trung tâm An ninh mạng quốc gia); các doanh nghiệp cung cấp dịch vụ viễn thông, internet; doanh nghiệp cung cấp dịch vụ an ninh mạng (nếu có); các cơ quan, đơn vị chức năng có liên quan.

- Thời gian thực hiện: Hằng năm.

b) Triển khai nhiệm vụ nhằm phòng ngừa sự cố và phát hiện sớm sự cố.

- Nội dung thực hiện: Thực hiện nghiêm công tác giám sát, phát hiện sớm nguy cơ, sự cố; kiểm tra, đánh giá an ninh mạng và rà quét, bóc gỡ, phân tích, xử lý mã độc; phòng ngừa sự cố, quản lý rủi ro; nghiên cứu, phân tích, xác minh, cảnh báo sự cố, rủi ro an ninh mạng, phần mềm độc hại; xây dựng, áp dụng quy trình, quy định, tiêu chuẩn an ninh mạng; tuyên truyền, nâng cao nhận thức về nguy cơ, sự cố, tấn công mạng.

- Đơn vị chủ trì: Công an tỉnh; Đơn vị quản lý, vận hành hệ thống thông tin; Đội ứng cứu sự cố; Sở Khoa học và Công nghệ.

- Đơn vị phối hợp: cơ quan điều phối quốc gia (Trung tâm An ninh mạng quốc gia); các cơ quan, đơn vị chức năng có liên quan.

- Thời gian thực hiện: Thường xuyên, hằng năm.

c) Các nội dung, nhiệm vụ nhằm bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố.

- Nội dung thực hiện: Mua sắm, nâng cấp, gia hạn bản quyền trang thiết bị, phần mềm, công cụ, phương tiện phục vụ ứng cứu, khắc phục sự cố; chuẩn bị các điều kiện bảo đảm, dự phòng nhân lực, vật lực, tài chính để sẵn sàng đối phó, ứng cứu, khắc phục khi sự cố xảy ra; tổ chức hoạt động của đội ứng cứu sự cố, bộ phận ứng cứu sự cố; thuê dịch vụ kỹ thuật và tổ chức, duy trì đội chuyên gia ứng cứu sự cố; tổ chức và tham gia các hoạt động của mạng lưới ứng cứu sự cố.

- Đơn vị chủ trì: Công an tỉnh; các sở, ban, ngành, đoàn thể của tỉnh; UBND các xã, phường; Đội ứng cứu sự cố.

- Đơn vị phối hợp: Cơ quan điều phối quốc gia (Trung tâm An ninh mạng quốc gia); các cơ quan, đơn vị chức năng có liên quan.

- Thời gian thực hiện: Hằng năm.

IV. KINH PHÍ THỰC HIỆN

Nguồn kinh phí thực hiện Kế hoạch được bố trí từ nguồn ngân sách nhà nước theo phân cấp ngân sách hiện hành; lồng ghép với kinh phí thực hiện các chương trình, kế hoạch, đề án khác có liên quan và các nguồn kinh phí hợp pháp khác theo quy định của pháp luật.

V. TỔ CHỨC THỰC HIỆN

1. Công an tỉnh – Cơ quan thường trực Tiểu ban An ninh mạng

- Là cơ quan đầu mối, chuyên trách về ứng cứu sự cố an ninh mạng trên địa bàn tỉnh, có trách nhiệm xây dựng và triển khai Kế hoạch này; tổ chức theo dõi, đôn đốc, phối hợp với các cơ quan, đơn vị, doanh nghiệp trong việc triển khai thực hiện Kế hoạch. Định kỳ 06 tháng, hằng năm hoặc đột xuất tổng hợp báo cáo kết quả thực hiện gửi UBND tỉnh, Trung tâm An ninh mạng quốc gia để theo dõi, chỉ đạo.

- Hằng năm tham mưu Tỉnh ủy ban hành quyết định kiện toàn Đội ứng cứu sự cố cho phù hợp với tình hình đảm bảo an ninh mạng trên địa bàn tỉnh Bắc Ninh.

- Tham mưu, tổ chức thực thi, đôn đốc, kiểm tra, đánh giá, giám sát, hướng dẫn công tác bảo đảm an ninh mạng định kỳ hằng năm hoặc theo chỉ đạo của Tỉnh ủy, UBND tỉnh đối với các cơ quan, đơn vị, doanh nghiệp trên địa bàn tỉnh. Tiến hành xử lý theo quy định của pháp luật các cá nhân, cơ quan vi phạm trong công tác bảo đảm an ninh mạng.

- Thẩm định, phê duyệt hoặc cho ý kiến về mặt chuyên môn đối với hồ sơ đề xuất cấp độ an toàn hệ thống thông tin theo thẩm quyền quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/07/2016 của Thủ tướng Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ và theo hướng dẫn tại Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP.

- Xây dựng nội dung, lập dự toán kinh phí bảo đảm cho hoạt động của Đơn vị chuyên trách ứng cứu sự cố và Đội ứng cứu sự cố.

2. Các cơ quan, ban, ngành, đoàn thể trong hệ thống chính trị của tỉnh

- Phân công lãnh đạo phụ trách, thành lập hoặc chỉ định bộ phận đầu mối chịu trách nhiệm về an ninh mạng tại cơ quan, đơn vị, địa phương theo thẩm quyền quản lý.

- Thực hiện đánh giá, xác định cấp độ, lập hồ sơ đề xuất cấp độ an toàn hệ thống thông tin theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Thủ tướng Chính phủ và Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ

trưởng Bộ Thông tin và Truyền thông.

- Xây dựng, cập nhật phương án ứng phó sự cố, bảo đảm an ninh mạng đối với mỗi hệ thống thông tin do cơ quan, đơn vị quản lý, vận hành gửi kết quả về Công an tỉnh (qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao **trước ngày 15/12 hằng năm)** để tổng hợp, báo cáo các cơ quan cấp trên theo quy định.

- Thực hiện bố trí cán bộ, công chức, viên chức chuyên trách về an ninh mạng tại cơ quan, đơn vị, địa phương mình; kịp thời thông báo về Công an tỉnh khi có sự thay đổi cán bộ, công chức, viên chức chuyên trách về an ninh mạng tại cơ quan, đơn vị hoặc đang là thành viên tham gia Đội ứng cứu sự cố.

- Cử cán bộ tham gia các chương trình huấn luyện, diễn tập và khóa đào tạo, tập huấn về ứng cứu sự cố, bảo đảm an ninh mạng để nâng cao kỹ năng và công tác tham mưu, triển khai giám sát, bảo đảm an ninh mạng.

- Triển khai tổ chức tuyên truyền, phổ biến các văn bản quy phạm pháp luật, tài liệu hướng dẫn chuyên môn, các hoạt động liên quan đến đảm bảo an ninh mạng của tỉnh, của cơ quan đơn vị trên Trang thông tin điện tử, các phương tiện thông tin đại chúng: nội dung của Luật An ninh mạng; Nghị định số 85/2016/NĐ-CP; Thông tư số 12/2022/TT-BTTTT; các Công điện, Chỉ thị của Thủ tướng Chính phủ và các Chỉ thị, văn bản của Bộ Thông tin và Truyền thông...

- Định kỳ sơ kết 6 tháng (**trước ngày 15/6**), tổng kết hằng năm **(trước ngày 15/12)**, hoặc đột xuất báo cáo tình hình ứng phó sự cố, bảo đảm an ninh mạng tại cơ quan, đơn vị, địa phương về Công an tỉnh (qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) để tổng hợp báo cáo các cơ quan cấp trên theo quy định.

3. Sở Khoa học và Công nghệ

- Tổ chức triển khai, xây dựng, quản lý, vận hành hạ tầng mạng, trung tâm dữ liệu, hạ tầng, nền tảng, cơ sở dữ liệu dùng chung, phục vụ chuyển đổi số, ứng dụng công nghệ thông tin; phối hợp Công an tỉnh trong thực hiện công tác đảm bảo an ninh mạng đối với hệ thống thông tin tập trung, dùng chung của tỉnh.

- Cử cán bộ có trình độ, kinh nghiệm tham gia xử lý, ứng cứu các sự cố về an ninh mạng, an ninh mạng xảy ra trên địa bàn tỉnh Bắc Ninh khi có yêu cầu của đơn vị điều phối.

- Trao đổi kịp thời cho Công an tỉnh mọi thông tin liên quan đến các sự cố an ninh mạng đối với hệ thống thông tin tập trung, dùng chung của tỉnh.

- Phối hợp Công an tỉnh phát huy thế mạnh về truyền thông cũng như các hệ thống thông tin sẵn có (Fanpage, email, Trang/Cổng thông tin điện tử...) phục vụ triển khai hiệu quả công tác tuyên truyền, phổ biến pháp luật về an ninh mạng, an

ninh mạng.

4. Sở Tài chính

- Hằng năm, căn cứ khả năng cân đối ngân sách, chủ trì, phối hợp với Công an tỉnh và các cơ quan, đơn vị có liên quan tham mưu cấp có thẩm quyền bố trí kinh phí theo phân cấp ngân sách nhà nước hiện hành.

- Thực hiện việc rà soát, kiểm tra, hướng dẫn thực hiện nhiệm vụ, dự án hoặc các chương trình, kế hoạch hằng năm của tỉnh về công tác ứng phó sự cố, bảo đảm an ninh mạng có sử dụng nguồn đầu tư công theo đúng quy định pháp luật hiện hành.

Trong quá trình thực hiện có nội dung cần trao đổi, các cơ quan, đơn vị, địa phương kịp thời trao đổi với Công an tỉnh – Cơ quan thường trực Tiểu ban An ninh mạng (cử đồng chí Nguyễn Hoàng Long, Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, số điện thoại 0968.859.168 làm đầu mối) để tổng hợp, hướng dẫn xử lý theo thẩm quyền hoặc báo cáo, tham mưu Bí thư Tỉnh ủy, Chủ tịch UBND tỉnh xem xét giải quyết theo đúng quy định pháp luật./.

GIÁM ĐỐC CÔNG AN TỈNH
kiêm
PHÓ TRƯỞNG TIỂU BAN TT

TỈNH ỦY BẮC NINH

Bùi Duy Hưng

Nơi nhận:
- BCĐ ANMQG (qua Cục A05, BCA) *(báo cáo)*,
- Bí thư Tỉnh ủy – Trưởng Tiểu ban *(báo cáo)*,
- Thường trực Tỉnh ủy, HĐND, UBND tỉnh,
- Ủy ban Mặt trận Tổ quốc tỉnh,
- Các ban, cơ quan, đơn vị thuộc Tỉnh ủy, UBND tỉnh,
- Công an tỉnh, Bộ CHQS tỉnh,
- Cơ quan Trung ương trên địa bàn,
- Đảng ủy, HĐND, UBND các xã, phường,
- Lưu: Văn phòng Tỉnh ủy, Công an tỉnh.

QUY TRÌNH TỔNG THỂ HỆ THỐNG PHƯƠNG ÁN ỨNG CỨU SỰ CỐ AN TOÀN THÔNG TIN MẠNG

(Đối với chủ quản hệ thống thông tin cấp sở, ban, ngành, địa phương, ban hành kèm theo Kế hoạch số 11-KH/TBANM ngày 29/5/2026 của Tiểu ban An ninh mạng tỉnh Bắc Ninh)