

Số: /KH-STC

Ninh Bình, ngày tháng 12 năm 2025

KẾ HOẠCH

Ứng phó sự cố, bảo đảm an toàn thông tin mạng trong hoạt động của Sở Tài chính tỉnh Ninh Bình

Thực hiện Kế hoạch số 119/KH-UBND ngày 24/10/2025 của UBND tỉnh Ninh Bình về việc Ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Ninh Bình; Căn cứ tình hình thực tế và chức năng, nhiệm vụ, Sở Tài chính ban hành Kế hoạch Ứng phó sự cố, bảo đảm an toàn thông tin mạng trong hoạt động của Sở Tài chính tỉnh Ninh Bình, như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Bảo đảm an toàn thông tin cho các hệ thống thông tin quan trọng tại Sở Tài chính; bảo đảm khả năng thích ứng chủ động, linh hoạt và giảm thiểu các nguy cơ, đe dọa mất an toàn thông tin trên 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 mất an toàn thông tin mạng.
- Tạo chuyển biến mạnh mẽ trong nhận thức về an toàn thông tin mạng đối với cán bộ, công chức, viên chức tại Sở.
- Bảo đảm 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 toàn thông tin mạng.

2. Yêu cầu

- Các hệ thống thông tin tại đơn vị phải được đánh giá hiện trạng và khả năng bảo đảm an toàn thông tin (ATTT) 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 ATTT mạng phải chuyển từ bị động sang chủ động, bao gồm: chủ động thực hiện sẵn lòng mỗi 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 ATTT 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 Ứng cứu khẩn cấp không gian mạng Việt Nam - VNCERT).

3. Quy định chung

a) Phạm vi và đối tượng

Kế hoạch này để ứng phó sự cố, bảo đảm an toàn thông tin mạng đối với các hệ thống thông tin của Sở Tài chính tỉnh Ninh Bình.

b) Nguyên tắc, phương châm ứng phó sự cố

- Tuân thủ các quy định pháp luật về điều phối, ứng cứu sự cố ATTT mạng.
- Chủ động, kịp thời, nhanh chóng, chính xác; phối hợp chặt chẽ, đồng bộ và hiệu quả giữa các phòng, đơn vị.
- 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 ứng phó sự cố ATTT mạng 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.

c) Các lực lượng tham gia ứng phó sự cố

- Các phòng, đơn vị thuộc Sở.
- Cá nhân là công chức, viên chức và người lao động của các phòng trực thuộc Sở và các đơn vị khác liên quan.
- Đội ứng cứu sự cố ATTT mạng của Sở (lực lượng chính ứng phó sự cố, trong đó Văn phòng là bộ phận thường trực).
- Doanh nghiệp cung cấp dịch vụ viễn thông internet (VNPT, Viettel,...).
- Doanh nghiệp cung cấp dịch vụ ATTT mạng (trường hợp thuê dịch vụ).
- Trong trường hợp cần thiết, mời các cơ quan đơn vị khác có chức năng về ứng cứu sự cố cùng tham gia.

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

- Văn phòng: Đơn vị chuyên trách ứng cứu sự cố ATTT mạng của Sở Tài chính; thực hiện chỉ đạo, tổ chức triển khai hoạt động ứng phó sự cố ATTT mạng và các nhiệm vụ khác khi xảy ra sự cố.
- Các phòng, đơn vị thuộc Sở: Lực lượng chính tham gia các hoạt động ứng cứu sự cố ATTT mạng tại Sở Tài chính.
- Trung tâm Chuyển đổi số và Truyền thông (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 Dữ liệu tỉnh; tham gia Đội ứng cứu sự cố ATTT mạng của tỉnh; xử lý, ứng cứu các sự cố về an toàn thông tin, an ninh mạng xảy ra trên địa bàn tỉnh khi có yêu cầu của đơn vị điều phối.
- Các cơ quan, đơn vị: Triển khai các nhiệm vụ theo chức năng, nhiệm vụ của đơn vị quản lý, vận hành hệ thống thông tin; Phối hợp với đơn vị chuyên trách ứng cứu sự cố ATTT mạng của tỉnh (Công an 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 ATTT 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 Sở Tài chính trong công tác ứng phó, xử lý các sự cố ATTT liên quan đến hạ tầng viễn thông, dịch vụ Internet do mình cung cấp hoặc quản lý.

II. NỘI DUNG THỰC HIỆN

1. Đánh giá các nguy cơ, sự cố ATTT mạng

a) Nội dung thực hiện: Đánh giá hiện trạng và khả năng bảo đảm ATTT mạng của hệ thống thông tin và các đối tượng cần bảo vệ; đánh giá, 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: Văn phòng

- Đơn vị phối hợp: các phòng đơn vị thuộc Sở 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 sẵn lòng mỗi 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 (thực hiện theo quy định tại Chỉ thị số 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ).

- Đơn vị chủ trì: Văn phòng

- Đơn vị phối hợp: các phòng đơn vị thuộc Sở và các cơ quan, đơn vị khác có liên quan.

- Thời gian thực hiện: Thường xuyên.

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

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

Đối với mỗi hệ thống thông tin, chương trình ứng dụng, Sở Tài chính 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, bảo đảm 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 c, Phần 2. 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.
- Sự cố liên quan đến các thiên tai, thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn và các sự cố gây mất ATTT 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 ATTT;
 - + 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 gây mất ATTT mạng khác.

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

- Đơn vị chủ trì: Văn phòng
- Đơn vị phối hợp: các phòng đơn vị thuộc Sở và các cơ quan, đơn vị khác có liên quan.
- Thời gian thực hiện: Thường xuyên hàng 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: Văn phòng
- Đơn vị phối hợp: các phòng đơn vị thuộc Sở và các cơ quan, đơn vị khác có liên quan.
- Thời gian thực hiện: Thường xuyên hàng năm.

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

a) Báo cáo sự cố ATTT mạng

- Đơn vị chủ trì: Văn phòng
- Đơn vị phối hợp: các phòng đơn vị thuộc Sở và các cơ quan, đơn vị khác có liên quan.
- Thời gian thực hiện: Ngay khi xảy ra sự cố và được duy trì trong suốt quá trình ứng cứu sự cố.

b) Tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố ATTT mạng

- Đơn vị chủ trì: Văn phòng
- Đơn vị phối hợp: các phòng đơn vị thuộc Sở và các cơ quan, đơn vị khác có 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 ATTT 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 và Điều 11 Thông tư 20/2017/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông

- Đơn vị chủ trì: Văn phòng
- Đơn vị phối hợp: các phòng đơn vị thuộc Sở và các cơ quan, đơn vị khác có liên quan.
- Thời gian thực hiện: Triển khai ngay sau khi tiếp nhận thông báo sự cố; cập nhật quy trình hàng năm hoặc khi có sự thay đổi.

III. KINH PHÍ THỰC HIỆN

Kinh phí thực hiện được bố trí trong dự toán ngân sách Nhà nước giao cho Sở Tài chính hằng năm.

IV. TỔ CHỨC THỰC HIỆN

1. Văn phòng

- Là đơn vị chủ trì, phối hợp với các phòng, đơn vị thuộc Sở triển khai thực hiện các nội dung tại Kế hoạch này.

- Là đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về ATTT mạng trong hoạt động của cơ quan.

- Chủ trì, phối hợp với các phòng, đơn vị thuộc Sở tiến hành kiểm tra công tác đảm bảo ATTT mạng định kỳ hàng quý hoặc theo hướng dẫn của cơ quan chuyên môn.

- Tham mưu đưa nội dung dự phòng kinh phí, nhân lực, vật lực thường trực sẵn sàng ứng cứu sự cố; triển khai điều hành, phối hợp tổ chức ứng cứu và thực hiện ứng cứu, xử lý, ngăn chặn, khắc phục sự cố vào các Kế hoạch về đảm bảo ATTT mạng, Kế hoạch chuyển đổi số hàng năm của cơ quan.

2. Các phòng, đơn vị trực thuộc Sở

Chủ động thông báo với Văn phòng khi phát hiện ra sự cố liên quan đến ATTT mạng đồng thời phối hợp với Văn phòng và các đơn vị liên quan thực hiện công tác ứng phó sự cố ATTT mạng tại phòng, đơn vị mình.

Trên đây là Kế hoạch Ứng phó sự cố, bảo đảm an toàn thông tin mạng trong hoạt động của Sở Tài chính tỉnh Ninh Bình; trong quá trình triển khai thực hiện kế hoạch nếu có khó khăn, vướng mắc, đề nghị Trưởng các phòng, đơn vị thuộc Sở phản ánh kịp thời về Văn phòng để tổng hợp, báo cáo Giám đốc Sở xem xét sửa đổi, bổ sung cho phù hợp./.

Nơi nhận:

- UBND tỉnh (để báo cáo);
- Công an tỉnh (để tổng hợp);
- Các phòng, đơn vị thuộc Sở;
- Trang TTĐT Sở Tài chính;
- Lưu: VT, VP.HL.

GIÁM ĐỐC

Mai Văn Quyết

