

KẾ HOẠCH
Ứng phó sự cố, bảo đảm an toàn thông tin mạng
Ngành Nông nghiệp và Môi trường tỉnh Nghệ An

Thực hiện Kế hoạch số 775/KH-UBND ngày 19/9/2025 của Ủy ban nhân dân tỉnh về việc ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Nghệ An; Sở Nông nghiệp và Môi trường xây dựng Kế hoạch thực hiện ứng phó sự cố, bảo đảm an toàn thông tin mạng như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Bảo đảm an toàn thông tin (ATTT) cho các hệ thống thông tin (HTTT) quan trọng trên địa bàn tỉnh; bảo đảm khả năng thích ứng một cách chủ động, linh hoạt và giảm thiểu các nguy cơ đe dọa mất ATTT trên mạng; đề ra các giải pháp ứng phó khi gặp sự cố mất ATTT mạng.
- Tạo chuyển biến mạnh mẽ trong nhận thức về ATTT đối với lực lượng cán bộ, công chức, viên chức trong các cơ quan nhà nước tỉnh.
- Xây dựng đội ứng cứu sự cố có đủ kiến thức, kỹ năng xử lý sự cố ATTT mạng đảm bảo linh hoạt, hiệu quả, phù hợp với yêu cầu thực tế.
- 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 ATTT mạng.

2. Yêu cầu

- Các HTTT của các đơn vị thuộc sở phải được đánh giá hiện trạng và khả năng bảo đảm ATTT mạng, dự báo các nguy cơ, sự cố mất ATTT mạng của HTTT của các đơn vị 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 HTTT trong phạm vi quản lý.
- Xác định cụ thể các nguồn lực đảm bảo, giải pháp tổ chức thực hiện và kinh phí để triển khai các nội dung của Kế hoạch, đảm bảo khả thi, hiệu quả.
- Thường xuyên trao đổi thông tin, chia sẻ kinh nghiệm trong công tác bảo đảm ATTT giữa các phòng, đơn vị; 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*).

II. CÁC QUY ĐỊNH CHUNG

1. Phạm vi và đối tượng

Kế hoạch này để ứng phó sự cố, bảo đảm ATTT mạng đối với các HTTT của Sở, các đơn vị thuộc Sở.

2. 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, đồng bộ và hiệu quả giữa các cơ quan, 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 HTTT.
- Tuân thủ các điều kiện, nguyên tắc ưu tiên về duy trì hoạt động của HTTT đã được cấp thẩm quyền phê duyệt trong kế hoạch ứng phó sự cố.
- 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 biết được 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.
- Công tác ứng phó sự cố ATTT mạng phải tuân thủ theo Quy trình ứng cứu sự cố thông thường quy định tại Phụ lục II kèm theo Thông tư số 20/2017/TT-BTTTT, Quy chế hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh và các văn bản quy định khác có liên quan.

3. Các lực lượng tham gia ứng phó sự cố

- Sở và đơn vị thuộc Sở.
- Đội ứng cứu sự cố An ninh mạng tỉnh (*lực lượng chính thực hiện công tác ứng phó sự cố, trong đó Công an tỉnh là cơ quan thường trực*).
- Chủ quản HTTT; đơn vị quản lý, vận hành HTTT.
- Trung tâm Khoa học Công nghệ và Truyền thông thuộc Sở Khoa học và Công nghệ.
- Doanh nghiệp cung cấp dịch vụ viễn thông internet (*VNPT, Viettel, FPT, Mobifone...*).
- Doanh nghiệp cung cấp dịch vụ ATTT mạng (*trường hợp thuê dịch vụ*).
- Trong trường hợp cần thiết, mời các cơ quan Trung ương có chức năng cùng tham gia.

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

- Các phòng, đơn vị: Có trách nhiệm cử cán bộ, công chức, viên chức phụ trách ATTT tham gia Đội ứng cứu sự cố an ninh mạng của Sở khi xử lý sự cố. Phối hợp với các đơn vị chuyên trách ứng cứu sự cố ATTT mạng của tỉnh (Công an tỉnh) và doanh nghiệp cung cấp, xây dựng HTTT trong công tác ứng phó, xử lý các sự cố.
- Sở Nông nghiệp và Môi trường: Lực lượng chính tham gia hoạt động ứng cứu sự cố ATTT mạng tỉnh, thực hiện nhiệm vụ xử lý, ứng cứu các sự cố về an ninh mạng, ATTT xảy ra khi có yêu cầu ứng phó, xử lý các sự cố.

III. NỘI DUNG THỰC HIỆN

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

1.1 Nội dung thực hiện: Đánh giá hiện trạng và khả năng bảo đảm ATTT mạng của các HTTT và các đối tượng cần bảo vệ thuộc phạm vi của Kế hoạch; đánh giá, dự báo các nguy cơ, sự cố tấn công mạng có thể xảy ra với các HTTT và các đối tượng cần bảo vệ; đánh giá dự báo các hậu quả, thiệt hại, tác động có thể có 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 nhà thầu đã ký hợp đồng cung cấp dịch vụ nếu có).

Đơn vị thực hiện: Đơn vị quản lý, vận hành HTTT; đơn vị quản lý, vận hành HTTT, phối hợp với Sở Nông nghiệp và Môi trường, đơn vị chuyên trách ứng cứu sự cố ATTT mạng của tỉnh (Công an tỉnh), Doanh nghiệp cung cấp dịch vụ ATTT (trường hợp thuê dịch vụ) và các đơn vị có liên quan.

Thời gian thực hiện: Thường xuyên

1.2 Nội dung thực hiện: Chủ động thực hiện sẵn lòng mỗi nguy hại và rà quét lỗ hổng trên các HTTT 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 thực hiện: Đơn vị quản lý, vận hành HTTT; đơn vị quản lý, vận hành HTTT, phối hợp với Sở Nông nghiệp và Môi trường, đơn vị chuyên trách ứng cứu sự cố ATTT mạng của tỉnh (Công an tỉnh), Doanh nghiệp cung cấp dịch vụ ATTT (trường hợp thuê dịch vụ) và các đơn vị có liên quan.

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 HTTT, 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 cần bảo đảm các nội dung sau:

2.1. Quy trình triển khai và các bước ưu tiên ứng cứu ban đầu khi HTTT 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.

2.2. 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 thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn và các sự cố gây mất ATTT mạng khác.

2.3. Phương án đối phó, ứng cứu, khắc phục sự cố đối với một hoặc nhiều tình huống sau:

- 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 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 HTTT;
 - + 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 thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn và các sự cố gây mất ATTT mạng khác.

2.4. Phương án 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 thực hiện: Đơn vị quản lý, vận hành HTTT, phối hợp với Sở Nông nghiệp và Môi trường, đơn vị chuyên trách ứng cứu sự cố ATTT mạng của tỉnh (Công an tỉnh), Doanh nghiệp cung cấp dịch vụ ATTT (trường hợp thuê dịch vụ) và các đơn vị 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

3.1. Thông báo, báo cáo sự cố ATTT mạng

Đơn vị thực hiện: Đơn vị quản lý, vận hành HTTT báo cáo Cơ quan chủ quản HTTT; Công an tỉnh; Đội ứng cứu sự cố an ninh mạng của tỉnh; 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.

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

Đơn vị thực hiện: Đơn vị quản lý, vận hành HTTT, phối hợp với Sở Nông nghiệp và Môi trường, đơn vị chuyên trách ứng cứu sự cố ATTT mạng của tỉnh (Công an tỉnh), Doanh nghiệp cung cấp dịch vụ ATTT (trường hợp thuê dịch vụ) và các đơn vị có liên quan.

3.3 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 số 20/2017/TT-BTTTT của Bộ.

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

4.1 Tham gia các chương trình huấn luyện, diễn tập: Tham gia các lớp diễn tập các phương án đối phó, ứng cứu sự cố tương ứng với các kịch bản, tình huống sự cố cụ thể do Cơ quan điều phối quốc gia, Công an tỉnh, Đội ứng cứu sự cố của tỉnh tổ chức.

4.2 Triển khai nhiệm vụ phòng ngừa sự cố và phát hiện sớm sự cố

Thực hiện nghiêm túc công tác giám sát, phát hiện sớm nguy cơ, sự cố, kiểm tra, đánh giá ATTT 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 ATTT mạng, chuẩn phần mềm độc hại; áp dụng quy trình, quy định, tiêu chuẩn ATTT; tuyên truyền nâng cao nhận thức về nguy cơ, sự cố, tấn công mạng.

Đơn vị thực hiện: Đơn vị quản lý, vận hành HTTT, phối hợp với Sở Nông nghiệp và Môi trường, đơn vị chuyên trách ứng cứu sự cố ATTT mạng của tỉnh (Công an tỉnh) và các đơn vị có liên quan.

Thời gian thực hiện: Hàng năm, thường xuyên

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

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 sự cố xảy ra; tổ chức hoạt động đội ứng cứu sự cố bộ phận; tham gia các hoạt động của mạng lưới ứng cứu sự cố.

Đơn vị thực hiện: Đơn vị quản lý, vận hành HTTT.

Thời gian thực hiện: Hàng năm

Kinh phí thực hiện Kế hoạch này được sử dụng 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 khác theo quy định của pháp luật.

IV. TỔ CHỨC THỰC HIỆN

1. Các đơn vị thuộc sở

- Phân công lãnh đạo phụ trách, thành lập hoặc chỉ định bộ phận đầu mối chịu trách nhiệm về ATTT mạng tại đơn vị theo thẩm quyền quản lý

- Thực hiện bố trí cán bộ, công chức, viên chức chuyên trách hoặc kiêm nhiệm ATTT mạng tại đơn vị mình; kịp thời thông báo về Sở Nông nghiệp và Môi trường khi có sự thay đổi cán bộ, công chức, viên chức chuyên trách hoặc kiêm nhiệm ATTT mạng của đơn vị mình.

- Xây dựng nội dung, lập dự toán kinh phí thực hiện các nhiệm vụ về ứng phó sự cố, bảo đảm ATTT mạng tại đơn vị trình cấp thẩm quyền phê duyệt hàng năm.

- Thực hiện đánh giá, xác định cấp độ, lập hồ sơ đề xuất cấp độ an toàn HTTT theo quy định tại Điều 14, Điều 15 Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn HTTT theo cấp độ và Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về đảm bảo an toàn HTTT theo cấp độ (**hoàn thành trước ngày 25/11/2025** đối với hệ thống mạng nội bộ và các hệ thống khác đã triển khai thực hiện).

- Cử cán bộ, công chức, viên chức tham gia các khóa đào tạo, tập huấn, diễn tập ứng phó của Sở, cấp trên để nâng cao kỹ năng và công tác tham mưu triển khai đảm bảo ATTT mạng tại đơn vị.

- 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 bảo đảm ATTT mạng cho cán bộ công chức, viên chức và người lao động tại đơn vị mình, lồng ghép trong các cuộc họp, hội nghị của đơn vị, Cổng/trang thông tin điện tử, phương tiện thông tin đại chúng...: nội dung của Luật An toàn thông tin 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 Công an, Bộ Khoa học và Công nghệ,...

- Thực hiện các nhiệm vụ được giao theo Kế hoạch này. Định kỳ 06 tháng (trước ngày 15/6) và 01 năm (trước ngày 15/11) hoặc đột xuất báo cáo tình hình ứng phó sự cố, bảo đảm ATTT mạng tại đơn vị về Sở Nông nghiệp và Môi trường (qua Văn phòng sở).

2. Văn phòng sở

- Là đầu mối, chuyên trách về ứng cứu sự cố ATTT mạng của Sở, có trách nhiệm chủ trì, theo dõi, đôn đốc, phối hợp với Công an tỉnh và các đơn vị liên quan tổ chức triển khai thực hiện Kế hoạch này; định kỳ 6 tháng, 01 năm hoặc đột xuất tổng hợp báo cáo kết quả thực hiện gửi Công an tỉnh, UBND tỉnh theo quy định.

- Tham mưu thành lập Tổ giúp việc chuyển đổi số trong đó lồng ghép nhiệm vụ công tác đảm bảo ATTT.

- Tham mưu, tổ chức thực thi, đôn đốc, kiểm tra, đánh giá, giám sát và hướng dẫn công tác bảo đảm ATTT định kỳ hàng năm theo chỉ đạo của cấp trên.

- Tham mưu trình phê duyệt hồ sơ cấp độ đối với mạng LAN tại Cơ quan Sở Nông nghiệp và Môi trường; thẩm định, phê duyệt hoặc cho ý kiến đối với hồ sơ đề xuất cấp độ an toàn HTTT theo quy định tại Nghị định số 85/2016/NĐ-CP, Thông tư số 12/2022/TT-BTTTT.

- Xây dựng nội dung, lập dự toán kinh phí bảo đảm cho nhiệm vụ bảo đảm an toàn an ninh thông tin đối với HTTT của Sở.

- Chủ trì tham mưu, phối hợp với các đơn vị liên quan tổ chức các cuộc tập huấn nâng cao trình độ cho cán bộ công chức, viên chức và người lao động của Ngành về ATTT; Tham gia, cử cán bộ tham gia các lớp tập huấn, diễn tập do UBND tỉnh, Công an tỉnh và các đơn vị liên quan tổ chức.

- Chịu trách nhiệm về ATTT mạng tại Cơ quan Sở và hướng dẫn cho các đơn vị đảm bảo ATTT mạng tại đơn vị; kịp thời thông báo về Công an tỉnh khi có sự thay đổi cán bộ, công chức chuyên trách về ATTT mạng của Sở hoặc đang là thành viên tham gia Đội ứng cứu sự cố an ninh mạng tỉnh.

3. Trung tâm Công nghệ thông tin

- Triển khai các Hệ thống dùng chung được Sở giao chủ trì triển khai; phối hợp với Công an tỉnh trong thực hiện công tác bảo đảm ATTT và phê duyệt hồ sơ cấp độ.

- Cử cán bộ có trình độ, kinh nghiệm tham gia xử lý, ứng cứu các sự cố về an ninh mạng, ATTT xảy ra trong Ngành khi có yêu cầu của Sở.

4. Phòng Kế hoạch tài chính

Tham mưu cấp có thẩm quyền bố trí kinh phí thực hiện các nhiệm vụ theo phân cấp quản lý ngân sách hiện hành.

Trong quá trình triển khai thực hiện nếu có khó khăn, vướng mắc, các đơn vị thuộc Sở phản ánh về Sở Nông nghiệp và Môi trường (qua Văn phòng sở) để tổng hợp, báo cáo Giám đốc sở xem xét, giải quyết./.

Nơi nhận:

- UBND tỉnh (b/c);
- Công an tỉnh;
- Giám đốc sở (b/c);
- Lãnh đạo sở;
- Các phòng thuộc sở;
- Các đơn vị thuộc sở;
- Lưu VT, VP (Hoàn).

**KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC**

Võ Thị Nhung