BỘ CÔNG THƯƠNG **CỘNG HÒA XÃ HỘI C[illegible]CHỦ NGHĨA VIỆT NAM**
Độc lập - Tự [illegible]ạnh phúc

Số: 932 /QĐ-BCT *Hà Nội, ngày 20 tháng 4 năm 2026*

QUYẾT ĐỊNH
Về việc ban hành phương án, kịch bản ứng cứu sự cố cho hệ thống thông tin của Bộ Công Thương

BỘ TRƯỞNG BỘ CÔNG THƯƠNG

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Nghị định số 40/2025/NĐ-CP ngày 26 tháng 02 năm 2025 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Công Thương;

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 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;

Căn cứ Chỉ thị số 18/CT-TTg ngày 13 tháng 10 năm 2022 của Thủ tướng Chính phủ về đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng Việt Nam;

Căn cứ Quyết định số 2409/QĐ-BCT ngày 10 tháng 9 năm 2024 của Bộ Công Thương về việc ban hành quy chế An toàn thông tin mạng và An ninh mạng Bộ Công Thương;

Căn cứ Quyết định số 481/QĐ-BCT ngày 19 tháng 3 năm 2026 của Bộ trưởng Bộ Công Thương về việc kiện toàn Tiểu ban An toàn, an ninh mạng Bộ Công Thương;

Căn cứ Quyết định số 536/QĐ-BCT ngày 25 tháng 3 năm 2026 của Bộ trưởng Bộ Công Thương về việc ban hành Kế hoạch bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong hệ thống chính trị tại Bộ Công Thương;

Căn cứ Nghị quyết số 57-NQ/TW ngày 22 tháng 12 năm 2024 của Bộ Chính trị về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia;

Căn cứ Quyết định số 229-QĐ/TW ngày 10 tháng 01 năm 2025 của Bộ

Chính trị về thành lập Ban Chỉ đạo Trung ương về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số;

Căn cứ Chỉ thị số 57-CT/TW ngày 31 tháng 12 năm 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;

Căn cứ Kế hoạch số 04-KH/BCĐTW ngày 05 tháng 01 năm 2026 của Ban Chỉ đạo Trung ương về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số về Kế hoạch bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong hệ thống chính trị;

Theo đề nghị của Cục trưởng Cục Thương mại điện tử và Kinh tế số.

QUYẾT ĐỊNH:

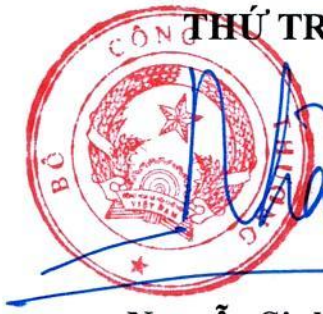
Điều 1. Ban hành kèm theo Quyết định này Phương án, kịch bản ứng cứu sự cố cho hệ thống thông tin của Bộ Công Thương.

Điều 2. Quyết định này có hiệu lực từ ngày ký.

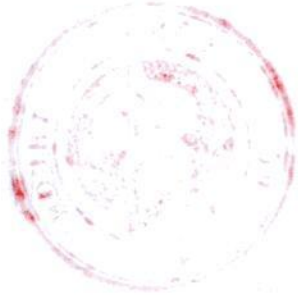
Điều 3. Chánh Văn phòng Bộ, Các thành viên Tiểu ban An toàn, an ninh mạng Bộ Công Thương, Thủ trưởng các đơn vị thuộc Bộ và các đơn vị, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Bộ trưởng (để báo cáo);
- Các Thứ trưởng;
- Lưu: VT, TMĐT$_{HoangDM}$

KT. BỘ TRƯỞNG
THỨ TRƯỞNG



Nguyễn Sinh Nhật Tân



BỘ CÔNG THƯƠNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

PHƯƠNG ÁN, KỊCH BẢN ỨNG CỨU SỰ CỐ CHO HỆ THỐNG THÔNG TIN CỦA BỘ CÔNG THƯƠNG

(Ban hành kèm theo Quyết định số 932/QĐ-TMĐT ngày 20 /4/2026 của Bộ trưởng Bộ Công Thương)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Phương án, kịch bản này quy định về việc phối hợp ứng phó sự cố an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các đơn vị thuộc Bộ Công Thương.

Điều 2. Đối tượng áp dụng

1. Các đơn vị thuộc Bộ Công Thương.

2. Cá nhân là cán bộ, công chức, viên chức, người lao động của cơ quan, đơn vị thuộc, trực thuộc Bộ Công Thương và các cá nhân khác liên quan.

Điều 3. Nguyên tắc, phương châm ứng phó sự cố

Sự cố an toàn thông tin mạng của hệ thống thông tin phải được tổ chức ứng phó khi xảy ra một trong các trường hợp sau:

1. Hệ thống bị gián đoạn dịch vụ.

2. Dữ liệu tuyệt mật hoặc bí mật nhà nước có khả năng bị tiết lộ.

3. Dữ liệu quan trọng của hệ thống không đảm bảo tính toàn vẹn và không có khả năng khôi phục.

4. Hệ thống bị mất quyền điều khiển.

5. Sự cố có khả năng xảy ra trên diện rộng hoặc gây ra các ảnh hưởng dây chuyền;

6. Đơn vị chủ quản hệ thống thông tin không đủ khả năng kiểm soát, xử lý được sự cố.

Điều 4. Chức năng, nhiệm vụ, trách nhiệm và cơ chế, quy trình phối hợp giữa các lực lượng tham gia ứng cứu sự cố

1. Cục Thương mại điện tử và Kinh tế số là đơn vị đầu mối, chủ trì công tác ứng cứu sự cố an toàn thông tin mạng của Bộ Công Thương; có trách nhiệm tổ

chức, điều phối và tham gia ứng cứu khẩn cấp nhằm bảo đảm an toàn thông tin mạng trong phạm vi Bộ Công Thương khi có yêu cầu.

2. Các đơn vị thuộc Bộ Công Thương có trách nhiệm:

a) Cử cán bộ, công chức phụ trách an toàn thông tin tham gia phối hợp ứng cứu sự cố khi được yêu cầu;

b) Chủ động phối hợp với Cục Thương mại điện tử và Kinh tế số trong việc phát hiện, báo cáo và xử lý sự cố thuộc phạm vi quản lý.

Chương II
ĐÁNH GIÁ CÁC NGUY CƠ, SỰ CỐ AN TOÀN THÔNG TIN MẠNG

Điều 5. Đánh giá các nguy cơ, sự cố an toàn thông tin mạng

1. Đánh giá hiện trạng và khả năng bảo đảm an toàn thông tin mạng của các hệ thống thông tin và các đối tượng cần bảo vệ.

2. Đánh giá, dự báo các nguy cơ, sự cố, tấn công mạng có thể xảy ra đối với các hệ thống thông tin và các đối tượng cần bảo vệ.

3. Đánh giá, dự báo hậu quả, thiệt hại và mức độ tác động có thể xảy ra khi phát sinh sự cố.

4. Đánh giá hiện trạng phương tiện, trang thiết bị, công cụ hỗ trợ và nguồn nhân lực phục vụ công tác phòng ngừa, ứng phó và khắc phục sự cố.

5. Các nguy cơ mất an toàn thông tin bao gồm

a) Nguy cơ mất an toàn thông tin về khía cạnh vật lý

Phát sinh từ các yếu tố như mất điện, điều kiện môi trường không bảo đảm (nhiệt độ, độ ẩm), hỏa hoạn, thiên tai hoặc thiết bị phần cứng bị hư hỏng, phá hoại.

b) Nguy cơ mất, hỏng hoặc bị sửa đổi nội dung thông tin

Người sử dụng có thể vô tình để lộ thông tin xác thực hoặc thao tác không đúng quy trình, tạo điều kiện để đối tượng xấu khai thác, đánh cắp hoặc làm sai lệch dữ liệu. Ngoài ra, đối tượng tấn công có thể sử dụng các công cụ, kỹ thuật để thay đổi nội dung thông tin nhằm làm sai lệch thông tin của chủ sở hữu hợp pháp.

c) Nguy cơ bị tấn công bởi phần mềm độc hại

Hệ thống có thể bị xâm nhập thông qua các loại phần mềm độc hại như vi-rút, sâu máy tính, phần mềm gián điệp và các biến thể khác với mục đích phá hoại, đánh cắp hoặc kiểm soát thông tin.

d) Nguy cơ bị xâm nhập từ lỗ hổng bảo mật

Lỗ hổng có thể phát sinh do lỗi lập trình, lỗi phần mềm hoặc cấu hình không an toàn trong hệ điều hành hoặc các ứng dụng, tạo điều kiện cho đối tượng tấn công khai thác để xâm nhập hệ thống.

đ) Nguy cơ bị xâm nhập do lộ, lọt thông tin xác thực

Việc sử dụng và quản lý tài khoản, mật khẩu không đúng quy định như chia sẻ mật khẩu, lưu trữ không an toàn hoặc đặt mật khẩu yếu làm giảm hiệu quả bảo vệ hệ thống và tạo điều kiện cho hành vi truy cập trái phép.

e) Nguy cơ mất an toàn thông tin qua thư điện tử

Tấn công có chủ đích thông qua thư điện tử giả mạo có thể chứa tệp đính kèm hoặc liên kết độc hại, nhằm đánh cắp thông tin xác thực hoặc phát tán phần mềm độc hại.

g) Nguy cơ mất an toàn thông tin trong quá trình truyền tin

Trong quá trình trao đổi dữ liệu trên môi trường mạng, thông tin có thể bị chặn, nghe lén, thay đổi hoặc phá hoại bởi các đối tượng tấn công.

Chương III
PHƯƠNG ÁN ĐỐI PHÓ, ỨNG CỨU SỰ CỐ ĐỐI VỚI MỘT SỐ TÌNH HUỐNG, SỰ CỐ CỤ THỂ

Điều 6. Phân nhóm sự cố an toàn thông tin mạng

1. Sự cố an toàn thông tin mạng nghiêm trọng là sự cố đáp ứng đồng thời các tiêu chí sau:

a) Hệ thống thông tin bị sự cố là hệ thống thông tin của Bộ Công Thương hoặc của các đơn vị thuộc Bộ và xảy ra một trong các trường hợp sau:

- Dữ liệu quan trọng của hệ thống không bảo đảm tính toàn vẹn và không có khả năng khôi phục;

- Hệ thống bị chiếm quyền điều khiển;

Sự cố có khả năng xảy ra trên diện rộng hoặc gây ảnh hưởng dây chuyền, làm tổn hại đến các hệ thống thông tin khác;

- Các trường hợp nghiêm trọng khác có mức độ ảnh hưởng tương đương.

b) Đơn vị chủ quản hệ thống thông tin không đủ khả năng tự kiểm soát hoặc xử lý sự cố.

2. Sự cố an toàn thông tin mạng thông thường là các sự cố không thuộc quy định tại khoản 1 Điều này, bao gồm:

a) Sự cố do bị tấn công mạng;

b) Sự cố do lỗi hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật hoặc do lỗi đường truyền, dịch vụ lưu trữ;

c) Sự cố do lỗi thao tác của người quản trị hoặc người vận hành hệ thống.

Điều 7. Nguyên tắc, phương châm ứng phó sự cố

1. Bảo đảm an toàn thông tin trong phòng, chống mã độc và bảo mật hệ thống

a) Bảo mật dữ liệu: Cán bộ, công chức, viên chức và người lao động có trách nhiệm bảo mật dữ liệu nghiệp vụ trên thiết bị được giao quản lý. Việc chia sẻ dữ liệu trên mạng được thực hiện theo phân cấp và do bộ phận quản trị mạng quản lý.

b) Bảo mật truy cập: Các chương trình ứng dụng và tài nguyên hệ thống phải được thiết lập cơ chế xác thực phù hợp như mật khẩu, mã khóa bảo mật.

c) Bảo mật hệ thống mạng và truyền tin: Hệ thống mạng và đường truyền phải được áp dụng các biện pháp bảo mật cần thiết nhằm ngăn chặn truy cập trái phép. Bộ phận quản trị mạng có trách nhiệm thường xuyên theo dõi, kiểm tra, phát hiện và xử lý kịp thời các hành vi xâm nhập.

d) An toàn trong sử dụng thiết bị: Khi không sử dụng máy tính trong thời gian dài, người dùng phải tắt thiết bị hoặc thiết lập chế độ bảo vệ để bảo đảm an toàn dữ liệu.

e) Phòng, chống mã độc: Người sử dụng có trách nhiệm tuân thủ các biện pháp phòng, chống mã độc; thực hiện quét, kiểm tra đối với dữ liệu từ thiết bị lưu trữ bên ngoài trước khi sử dụng. Trường hợp phát hiện thiết bị nhiễm mã độc phải thực hiện cô lập khỏi mạng để tránh lây lan. Không truy cập vào liên kết hoặc tải tệp từ nguồn không rõ ràng.

2. Bảo đảm an toàn máy chủ, máy trạm và cơ chế sao lưu, phục hồi

a) Kiểm soát chặt chẽ việc cài đặt phần mềm trên máy chủ và máy trạm; các phần mềm phải được cập nhật bản vá bảo mật kịp thời. Triển khai các giải pháp phòng, chống mã độc và thiết lập cơ chế quét định kỳ.

b) Thực hiện sao lưu định kỳ đối với cơ sở dữ liệu và dữ liệu quan trọng; bản sao lưu phải được lưu trữ theo quy định nhằm phục vụ phục hồi hệ thống khi xảy ra sự cố.

3. Bảo đảm an toàn hệ thống mạng và kết nối Internet

a) Quản lý mạng nội bộ: Hệ thống mạng nội bộ được tổ chức theo mô hình phù hợp, có phân vùng mạng, kiểm soát truy cập và chỉ cho phép mở các dịch vụ

cần thiết.

b) Quản lý mạng không dây: Mạng không dây kết nối vào mạng nội bộ phải được cấu hình bảo mật, thiết lập cơ chế xác thực và thay đổi mật khẩu định kỳ.

c) Quản lý truy cập từ xa: Việc truy cập từ xa vào mạng nội bộ phải được kiểm soát chặt chẽ, đặc biệt đối với tài khoản quản trị; hạn chế truy cập từ các môi trường không an toàn.

4. Bảo đảm an toàn truy cập và quản lý tài khoản

a) Mỗi người dùng được cấp một tài khoản truy cập với định danh duy nhất; việc sử dụng tài khoản phải đúng chức năng, nhiệm vụ và bảo đảm không chia sẻ trái phép. Trường hợp sử dụng tài khoản dùng chung phải có cơ chế xác định trách nhiệm quản lý.

b) Mật khẩu truy cập hệ thống phải đáp ứng yêu cầu về độ phức tạp, có độ dài tối thiểu 8 ký tự và bao gồm các thành phần cần thiết theo quy định bảo mật.

5. Bảo đảm an toàn thông tin và dữ liệu

a) Thông tin, dữ liệu phải được bảo đảm các yêu cầu về tính toàn vẹn, tính bảo mật và tính sẵn sàng. Dữ liệu quan trọng khi lưu trữ hoặc trao đổi phải được áp dụng các biện pháp bảo vệ như mã hóa, xác thực và lưu trữ dự phòng.

b) Trong trao đổi thông tin phục vụ công việc, các đơn vị và cá nhân phải sử dụng hệ thống thư điện tử công vụ và các hệ thống thông tin do Bộ Công Thương cung cấp; hạn chế sử dụng các nền tảng công cộng không bảo đảm an toàn.

c) Việc bảo đảm an toàn thông tin phải tuân thủ quy chế bảo đảm an toàn thông tin mạng của Bộ Công Thương.

6. Thuê dịch vụ giám sát an toàn thông tin mạng

Triển khai thuê dịch vụ giám sát an toàn thông tin mạng theo quy định nhằm nâng cao năng lực phát hiện, cảnh báo và ứng phó sự cố

Điều 8. Quy trình ứng cứu sự cố an toàn thông tin mạng

Quy trình ứng cứu sự cố an toàn thông tin mạng được thực hiện theo các bước sau:

Bước 1. Thông báo sự cố

Cán bộ, công chức, viên chức, người lao động tại các đơn vị thuộc Bộ Công Thương khi phát hiện hoặc nghi ngờ xảy ra sự cố trong quá trình sử dụng hệ thống thông tin phải thông báo ngay cho bộ phận ứng cứu sự cố theo quy định.

Bước 2. Tiếp nhận sự cố

Bộ phận ứng cứu sự cố có trách nhiệm tiếp nhận thông tin về sự cố thông qua các phương thức như điện thoại, hệ thống thông tin, báo cáo trực tiếp hoặc các kênh phù hợp khác.

Bước 3. Xác minh, xác nhận sự cố

Bộ phận ứng cứu sự cố tiến hành xác minh, xác nhận sự cố trên cơ sở các nội dung sau:

a) Tình trạng sự cố (chưa xảy ra, đang xảy ra hoặc đã xảy ra);

b) Mức độ sự cố (nghiêm trọng hoặc thông thường);

c) Phạm vi ảnh hưởng (diện rộng, hệ thống mạng hoặc một thiết bị đơn lẻ);

d) Thời gian, địa điểm xảy ra sự cố và các thông tin liên quan khác.

Bước 4. Phân loại sự cố

Bộ phận ứng cứu sự cố thực hiện phân loại sự cố theo tính chất, bao gồm:

a) Sự cố do lỗi hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật hoặc lỗi đường truyền, dịch vụ lưu trữ;

b) Sự cố do lỗi của người quản trị hoặc người vận hành hệ thống;

c) Sự cố do tấn công mạng trong phạm vi hạn chế, có thể khắc phục;

d) Sự cố tấn công thay đổi giao diện (deface);

đ) Sự cố tấn công lừa đảo (phishing);

e) Sự cố tấn công phát tán mã độc (malware);

g) Sự cố tấn công từ chối dịch vụ (DoS/DDoS);

h) Sự cố có yếu tố nước ngoài cần phối hợp quốc tế;

i) Các sự cố khác có liên quan.

Bước 5. Báo cáo, xin ý kiến chỉ đạo và tổ chức ứng cứu

Ngay sau khi phân loại sự cố, bộ phận ứng cứu sự cố có trách nhiệm báo cáo lãnh đạo đơn vị để xem xét, chỉ đạo xử lý. Việc tổ chức ứng cứu được thực hiện như sau:

a) Trường hợp sự cố thông thường: Thông báo cho các đơn vị liên quan để triển khai xử lý theo quy trình ứng cứu sự cố thông thường quy định tại Phụ lục I (trích quy trình ứng cứu sự cố thông thường ban hành kèm theo Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của Bộ Thông tin và Truyền thông);

b) Trường hợp sự cố nghiêm trọng: Thực hiện báo cáo sự cố đến VNCERT/CC để phối hợp ứng cứu; đồng thời tổ chức triển khai lực lượng, huy động nguồn lực cần thiết, kích hoạt phương án ứng cứu khẩn cấp và thực hiện các bước tiếp theo theo quy định tại Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ.

Bước 6. Phối hợp xử lý, khắc phục và tổng kết sự cố

Bộ phận ứng cứu sự cố chủ trì hoặc phối hợp với các cơ quan, đơn vị liên quan thực hiện các hoạt động: thu thập thông tin phục vụ phân tích sự cố; phân tích, xác định nguyên nhân; xử lý, khắc phục sự cố; khôi phục hệ thống; kiểm tra, đánh giá mức độ an toàn sau xử lý; báo cáo, tổng kết và rút kinh nghiệm.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 9. Trách nhiệm của Cục Thương mại điện tử và Kinh tế số

1. Chủ trì, phối hợp với các đơn vị thuộc Bộ Công Thương tổ chức triển khai thực hiện các nội dung quy định tại Điều 5, Điều 6 và Điều 7 của Kịch bản này.

2. Là đầu mối tiếp nhận, tổ chức xử lý các sự cố an toàn thông tin mạng trong hoạt động của Bộ Công Thương.

3. Chủ trì, phối hợp với các đơn vị thuộc Bộ Công Thương tổ chức kiểm tra công tác bảo đảm an toàn thông tin mạng định kỳ hằng năm hoặc theo yêu cầu, hướng dẫn của cơ quan có thẩm quyền.

4. Chủ trì tham mưu xây dựng, bố trí nguồn lực phục vụ công tác bảo đảm an toàn thông tin mạng, bao gồm kinh phí, nhân lực và trang thiết bị; lồng ghép nội dung ứng cứu sự cố, phòng ngừa, xử lý và khắc phục sự cố vào các kế hoạch về bảo đảm an toàn thông tin mạng và kế hoạch ứng dụng công nghệ thông tin của Bộ Công Thương.

5. Tổ chức điều hành, phối hợp triển khai các hoạt động ứng cứu sự cố; huy động các lực lượng, nguồn lực cần thiết để kịp thời xử lý, ngăn chặn và khắc phục sự cố an toàn thông tin mạng khi xảy ra

Điều 10. Trách nhiệm của các đơn vị thuộc Bộ Công Thương

1. Tổ chức triển khai các biện pháp bảo đảm an toàn thông tin mạng đối với hệ thống thông tin thuộc phạm vi quản lý.

2. Chủ động trang bị, cài đặt và duy trì các giải pháp bảo đảm an toàn thông tin mạng như phần mềm phòng, chống mã độc, tường lửa và các công cụ bảo mật

cần thiết cho hệ thống máy tính, mạng và hệ thống thông tin của đơn vị.

3. Phối hợp với Cục Thương mại điện tử và Kinh tế số và các đơn vị liên quan trong việc phát hiện, thông báo, ứng phó, xử lý và khắc phục sự cố an toàn thông tin mạng tại đơn vị.

4. Kịp thời báo cáo sự cố an toàn thông tin mạng và cung cấp đầy đủ thông tin, dữ liệu cần thiết phục vụ công tác ứng cứu khi có yêu cầu.

5. Trong quá trình triển khai thực hiện Phương án, kịch bản này, trường hợp phát sinh khó khăn, vướng mắc, các đơn vị phản ánh về Cục Thương mại điện tử và Kinh tế số để tổng hợp, báo cáo Lãnh đạo Bộ xem xét, quyết định./.