



QUY CHẾ

Bảo đảm an toàn thông tin, an ninh mạng hệ đối với các hệ thống thông tin cấp độ 3 do Sở Công Thương tỉnh Hưng Yên quản lý, vận hành

(Ban hành kèm theo Quyết định số: 225/QĐ-SCT ngày 28/9/2026 của Sở Công Thương)

Chương I QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. Phạm vi điều chỉnh

Quy chế này quy định các chính sách quản lý và các biện pháp nhằm bảo đảm an toàn thông tin cho các hệ thống thông tin của Sở Công Thương, bao gồm phạm vi quản lý vật lý, logic, các ứng dụng, dịch vụ và nguồn nhân lực.

2. Đối tượng áp dụng

Các cán bộ, công chức thuộc các phòng, đơn vị thuộc Sở Công Thương và các tổ chức, cá nhân có kết nối, sử dụng hệ thống thông tin của Sở Công Thương.

Điều 2. Giải thích từ ngữ

Trong quy chế này, các từ ngữ dưới đây được hiểu như sau:

An toàn thông tin mạng: là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

Mạng: là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua mạng viễn thông và mạng máy tính.

Hệ thống thông tin: là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên mạng.

Chủ quản hệ thống thông tin: là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý về an toàn thông tin, cơ quan quản lý cấp trên là UBND tỉnh, Công an tỉnh Hưng Yên và Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao - Bộ Công an.

Điều 3. Mục tiêu, nguyên tắc bảo đảm an toàn thông tin

1. Mục tiêu bảo đảm an toàn thông tin

Bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn,

tính bảo mật và tính khả dụng của Hệ thống thông tin.

2. Nguyên tắc

a) Tổ chức, cá nhân thuộc đối tượng áp dụng Quy chế này có trách nhiệm bảo đảm an toàn thông tin và hệ thống thông tin trong phạm vi xử lý công việc của mình theo quy định của pháp luật, hướng dẫn của cơ quan, đơn vị có thẩm quyền và các quy định tại Quy chế này.

b) Bảo đảm an toàn thông tin (ATTT) là yêu cầu bắt buộc, phải được thực hiện thường xuyên, liên tục trong quá trình:

- Thu thập, tạo lập, xử lý, truyền tải, lưu trữ và sử dụng thông tin, dữ liệu.
- Thiết kế, thiết lập và vận hành, nâng cấp, hủy bỏ hệ thống thông tin.

c) Việc bảo đảm an toàn Hệ thống thông tin Sở Công Thương được thực hiện một cách tổng thể, đồng bộ, tập trung trong việc đầu tư các giải pháp bảo vệ, có sự dùng chung, chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư thừa, trùng lặp.

Điều 4. Những hành vi nghiêm cấm

Các hành vi bị nghiêm cấm quy định tại Điều 7 Luật An toàn thông tin mạng, cụ thể gồm:

1. Ngăn chặn việc truyền tải thông tin trên mạng, can thiệp, truy nhập, gây nguy hại, xóa, thay đổi, sao chép và làm sai lệch thông tin trên mạng trái pháp luật.
2. Gây ảnh hưởng, cản trở trái pháp luật tới hoạt động bình thường của hệ thống thông tin hoặc tới khả năng truy nhập hệ thống thông tin của người sử dụng.
3. Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của biện pháp bảo vệ an toàn thông tin mạng của hệ thống thông tin; tấn công, chiếm quyền điều khiển, phá hoại hệ thống thông tin.
4. Phát tán thư rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo.
5. Thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác; lợi dụng sơ hở, điểm yếu của hệ thống thông tin để thu thập, khai thác thông tin cá nhân.

6. Xâm nhập trái pháp luật bí mật mật mã và thông tin đã mã hóa hợp pháp của cơ quan, tổ chức, cá nhân; tiết lộ thông tin về sản phẩm mật mã dân sự, thông tin về khách hàng sử dụng hợp pháp sản phẩm mật mã dân sự; sử dụng, kinh doanh các sản phẩm mật mã dân sự không rõ nguồn gốc.

Điều 5. Phối hợp với những cơ quan/tổ chức có thẩm quyền

1. Bộ phận chuyên trách về an toàn thông tin

- Sở Công Thương chỉ định ít nhất 01 cán bộ là bộ phận chuyên trách chính về an toàn thông tin và 01 cán bộ dự phòng hoặc sẽ theo phân công nhiệm vụ trực tiếp của Sở Công Thương trong trường hợp thay thế, thực hiện nhiệm vụ tiếp

nhận, báo cáo, phối hợp, ứng cứu, xử lý sự cố về an toàn thông tin đối với Hệ thống thông tin Sở Công Thương.

- Bộ phận chuyên trách về an toàn thông tin có trách nhiệm tham gia đầy đủ các hoạt động phối hợp, đào tạo, tập huấn, các chương trình công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền.

2. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin:

Sở Công Thương giao Văn phòng Sở là đầu mối liên hệ, phối hợp các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin phục vụ việc bảo đảm an toàn, an ninh thông tin cho Hệ thống thông tin Sở Công Thương; tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin của Hệ thống mạng nội bộ; phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin.

- Người liên hệ: Ông Nguyễn Xuân Tuấn – Chánh Văn phòng Sở.

+ Số điện thoại: 0982193006

+ Email: Soct@hungyen.gov.vn

Điều 6. Bảo đảm nguồn nhân lực

1. Tuyển dụng

Công chức được tuyển dụng vào vị trí làm về an toàn thông tin (hoặc kiêm nhiệm) có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng.

2. Trong quá trình làm việc

a) Trách nhiệm bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống:

- Với người sử dụng:

+ Người sử dụng có trách nhiệm đảm bảo ATTT đối với từng vị trí công việc.

+ Phải được thường xuyên tổ chức quán triệt các quy định về ATTT, nhằm nâng cao nhận thức về trách nhiệm đảm bảo ATTT.

+ Phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp thiết bị.

- Với cán bộ quản lý và vận hành hệ thống

+ Cán bộ quản lý và vận hành hệ thống phải thiết lập phương pháp hạn chế truy cập mạng không dây, giám sát và điều khiển truy cập không dây, tổ chức sử dụng chứng thực và mã hóa để bảo vệ truy cập không dây tới hệ thống thông tin.

+ Cán bộ quản lý và vận hành hệ thống phải tổ chức quản lý định danh đối với tất cả người dùng tham gia sử dụng hệ thống thông tin.

b) Định kỳ hàng năm tổ chức hoặc tham gia phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin, an ninh mạng cho người sử dụng do đơn vị chức năng tổ chức.

3. Chấm dứt thay đổi công việc

a) Cán bộ chấm dứt hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của tổ chức.

b) Cán bộ nghỉ việc phải có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc.

c) Bộ phận chuyên trách thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc.

Chương II

BẢO ĐẢM AN TOÀN THÔNG TIN TRONG QUẢN LÝ THIẾT KẾ, XÂY DỰNG HỆ THỐNG THÔNG TIN

Điều 7. Thiết kế an toàn hệ thống thông tin

1. Bộ phận chuyên trách xây dựng tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin và thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống.

2. Bộ phận chuyên trách xây dựng tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống.

3. Bộ phận chuyên trách xây dựng tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ của hệ thống thông tin thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống.

4. Bộ phận chuyên trách xây dựng tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin của hệ thống thông tin thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống.

5. Bộ phận chuyên trách khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống, báo cáo Lãnh đạo quyết định trước khi thực hiện thay đổi.

Điều 8. Quản lý nhà cung cấp sản phẩm, dịch vụ

1. Lập và cập nhật danh sách các nhà cung cấp sản phẩm, dịch vụ định kỳ. Đơn vị vận hành xây dựng quy trình đánh giá nhà cung cấp sản phẩm, dịch vụ an ninh mạng sau đó đánh giá và cập nhật danh sách tối thiểu 01 lần/năm hoặc khi xảy ra thay đổi ảnh hưởng đến danh sách.

2. Rà soát vấn đề bảo mật khi kết thúc hợp đồng với các nhà cung cấp dịch vụ.

Điều 9. Phát triển phần mềm thuê khoán

1. Yêu cầu có biên bản, hợp đồng và các cam kết đối với bên thuê khoán các nội dung liên quan đến việc phát triển phần mềm thuê khoán.
2. Yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm:
 - a) Các nhà phát triển cung cấp mã nguồn phần mềm cho bộ phận chuyên trách.
 - b) Bộ phận chuyên trách có trách nhiệm quản lý và lưu trữ mã nguồn an toàn.

Điều 10. Thử nghiệm và nghiệm thu hệ thống

1. Bên triển khai xây dựng kế hoạch, nội dung thử nghiệm hệ thống trước khi thực hiện thử nghiệm và nghiệm thu hệ thống.
2. Đơn vị vận hành thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác theo phương án thiết kế được phê duyệt trong Hồ sơ đề xuất cấp độ.
3. Bộ phận chuyên trách và bên triển khai hệ thống xây dựng kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống, trình Lãnh đạo đơn vị phê duyệt trước khi đưa hệ thống vào vận hành, khai thác.
4. Bộ phận chuyên trách phối hợp với bên triển khai hệ thống thực hiện thử nghiệm và nghiệm thu hệ thống, trước khi đưa vào vận hành, khai thác.

Chương III

BẢO ĐẢM AN TOÀN THÔNG TIN TRONG QUẢN LÝ VẬN HÀNH HỆ THỐNG THÔNG TIN

Điều 11. Quản lý tài sản Công nghệ thông tin

1. Quản lý tài sản phần cứng và phần mềm: Lập danh sách, kiểm kê, rà soát và cập nhật danh sách cho tất cả tài sản thuộc hệ thống thông tin định kỳ 6 tháng/lần.
2. Xây dựng quy trình xử lý tài sản chưa được quản lý: Rà soát, xử lý tài sản phần cứng không có trong danh sách định kỳ tối thiểu 01 lần/tháng và phần mềm trái phép định kỳ tối thiểu 01 lần/quý.
3. Quản lý tài sản thông tin: Mức độ nhạy cảm của tài sản thông tin phải được phân loại thành: Công khai, Nội bộ, Hạn chế truy cập, và Bí mật nhà nước. Định kỳ kiểm tra cấp độ phân quyền dữ liệu tối thiểu 01 lần/tháng.

Điều 12. Quản lý tài khoản

1. Người sử dụng thực hiện quản lý tài khoản, mật khẩu được cấp; định kỳ 02 tháng đổi mật khẩu một lần. Mật khẩu phải đặt tối thiểu 8 ký tự, bao gồm chữ hoa, chữ thường, số và ký tự đặc biệt (Trường hợp quên mật khẩu thông báo cho phòng Chuyển đổi số - Cơ yếu, Văn phòng Tỉnh ủy để hỗ trợ khôi phục hoặc cấp mật khẩu mới).
2. Quản lý tách biệt giữa các loại tài khoản dùng trong hệ thống thông tin (quản trị, nghiệp vụ, kỹ thuật, dịch vụ).

3. Tài khoản được cấp cho người dùng để phục vụ công việc phải được quản lý chặt chẽ; khi người dùng chuyển công tác, nghỉ hưu hoặc thay đổi vị trí công tác, đơn vị quản lý có trách nhiệm kịp thời điều chỉnh quyền truy cập hoặc thu hồi (xóa/vô hiệu hóa) tài khoản. Đồng thời, các tài khoản không hoạt động phải được xóa hoặc vô hiệu hóa sau tối đa 45 ngày hoặc ngay khi có thay đổi về nhân sự quản lý tài khoản. Định kỳ tối thiểu 01 lần/năm, đơn vị thực hiện rà soát, đánh giá và cập nhật quy định, danh sách tài khoản nhằm bảo đảm an toàn thông tin.

4. Nghiêm cấm sử dụng tài khoản của người khác quản lý khi chưa có sự đồng ý của chủ tài khoản.

Điều 13. Quản lý an toàn mạng

1. Yêu cầu chung về kết nối hệ thống

a) Các mô hình, giải pháp kỹ thuật kết nối các hệ thống mạng máy tính với nhau phải tuân thủ Kiến trúc chuyển đổi số thống nhất trong các cơ quan và Nhà nước.

b) Hệ thống mạng phải được thiết kế thống nhất, bảo đảm khả năng kết nối, tích hợp, chia sẻ và tương tác giữa các hệ thống; thực hiện quản lý định danh, xác thực đối với toàn bộ người sử dụng nhằm bảo đảm quản lý chặt chẽ, an toàn, bảo mật.

c) Hoạt động của hệ thống mạng phải được giám sát thường xuyên, liên tục nhằm bảo đảm tính sẵn sàng, ổn định và khả dụng của hệ thống.

2. Tiêu chuẩn băng thông và chất lượng đường truyền

a) Đường truyền kết nối phải bảo đảm tốc độ tối thiểu:

10 Mbps đối với cấp cơ sở;

50 Mbps đối với cấp tỉnh.

b) Bảo đảm không tắc nghẽn, trong đó mức chiếm dụng băng thông trung bình không vượt quá 80% dung lượng tối đa của đường truyền.

3. Yêu cầu an toàn, bảo mật trong kết nối

a) Toàn bộ dữ liệu truyền qua mạng phải được mã hóa bằng giao thức bảo mật như VPN hoặc các giao thức khác theo hướng dẫn của cơ quan có thẩm quyền.

b) Dữ liệu thuộc danh mục bí mật nhà nước phải được mã hóa bằng giải pháp bảo mật theo quy định của cơ quan chuyên trách bảo mật, cơ yếu.

c) Triển khai thống nhất, đồng bộ các giải pháp giám sát an ninh mạng, phát hiện và phòng chống xâm nhập, mã độc trong toàn hệ thống.

d) Thiết lập các cơ chế kiểm soát truy cập từ bên ngoài và bên trong mạng; phân tách vùng mạng; phòng chống tấn công giữa các vùng mạng và lây lan mã độc.

đ) Cấu hình truy cập, quản trị hệ thống từ xa phải sử dụng các giao thức bảo mật có mã hóa như SSL/TLS, SSH, VPN hoặc các giải pháp tương đương.

4. Kết nối mạng diện rộng của Sở

Việc kết nối mạng cấp cơ sở vào mạng thông tin diện rộng của Sở phải sử dụng mạng truyền số liệu chuyên dùng phục vụ các cơ quan, Nhà nước; tuân thủ các quy định hiện hành về tiêu chuẩn kỹ thuật, chất lượng kênh truyền, mô hình và đối tượng kết nối.

5. Quản lý, vận hành và thay đổi cấu hình hệ thống mạng

a) Hệ thống mạng phải được cấu hình để:

- Kiểm soát truy cập từ bên ngoài và bên trong mạng;
- Kết nối về hệ thống giám sát tập trung;
- Phòng chống xâm nhập, mã độc;
- Bảo đảm an toàn thông tin trong quá trình vận hành.

b) Việc cài đặt, kết nối, thay đổi hoặc gỡ bỏ thiết bị mạng phải được sự cho phép của người có thẩm quyền và thực hiện theo quy trình được phê duyệt.

c) Khi thực hiện nâng cấp hoặc thay đổi cấu hình hệ thống phải thực hiện ngoài giờ làm việc và kiểm tra, đánh giá tổng thể hệ thống sau khi hoàn thành.

6. Sao lưu, dự phòng và khôi phục hệ thống

a) Định kỳ hàng tháng hoặc khi có thay đổi, thực hiện sao lưu, dự phòng hệ thống trên các phương tiện lưu trữ độc lập.

b) Dữ liệu phải được sao lưu bao gồm: cấu hình hệ thống, hệ điều hành máy chủ, cơ sở dữ liệu và dữ liệu nghiệp vụ.

c) Có phương án khôi phục hệ thống kịp thời khi xảy ra sự cố, bảo đảm duy trì hoạt động liên tục.

7. Quản lý truy cập và khai thác hệ thống

a) Cán bộ quản trị, vận hành chỉ được truy cập, khai thác hệ thống theo đúng chức năng, nhiệm vụ và quyền hạn được phân công; bảo đảm không tiết lộ thông tin ra bên ngoài khi chưa được phép.

b) Xây dựng và triển khai quy trình kết nối thiết bị đầu cuối vào hệ thống; kiểm soát chặt chẽ việc truy cập và sử dụng tài nguyên mạng.

8. Yêu cầu đối với thiết bị mạng

Các thiết bị trong hệ thống phải được cấu hình tối ưu, tăng cường bảo mật, ưu tiên sử dụng thiết bị chuyên dụng, bảo đảm đáp ứng yêu cầu an toàn thông tin trước khi đưa vào vận hành, khai thác.

Điều 14. Quản lý an toàn máy chủ và ứng dụng (khi được trang bị)

1. Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ:

a) Bảo đảm cho hệ điều hành, phần mềm cài đặt trên máy chủ hoạt động liên tục, ổn định và an toàn theo thiết kế.

b) Thường xuyên giám sát, kiểm tra cấu hình, các tệp nhật ký (log) hoạt động của hệ điều hành, phần mềm nhằm kịp thời phát hiện, cảnh báo và xử lý những sự cố hoặc hành vi truy cập trái phép.

c) Quản lý chặt chẽ các thay đổi cấu hình kỹ thuật của hệ điều hành, phần mềm; mọi sự thay đổi phải được ghi nhận vào nhật ký quản trị.

d) Có phương án và thực hiện cập nhật bản vá lỗi, xử lý điểm yếu an toàn thông tin cho hệ điều hành và các dịch vụ hệ thống trên máy chủ tối thiểu 01 lần/tháng hoặc ngay khi có cảnh báo nguy hiểm từ cơ quan chức năng.

đ) Các bản quyền phần mềm, chứng chỉ bảo mật (SSL/TLS) cần được thống kê, quản lý thời hạn phục vụ cho việc duy trì và gia hạn kịp thời.

2. Quy định đối với ứng dụng:

a) Hoạt động của ứng dụng phải được giám sát thường xuyên, liên tục, đảm bảo tính khả dụng và hiệu năng của ứng dụng.

b) Ứng dụng phải được thiết lập chính sách xác thực chặt chẽ (khuyến khích xác thực đa nhân tố đối với tài khoản quản trị); kiểm soát truy cập theo nguyên tắc quyền tối thiểu; có phương án mã hóa bảo mật thông tin liên lạc và biện pháp bảo vệ mã nguồn ứng dụng (chống các lỗi phổ biến như SQL Injection, XSS...).

c) Ứng dụng phải được kiểm tra, đánh giá an toàn thông tin trước khi đưa vào sử dụng, định kỳ tối thiểu 01 năm/lần (đối với hệ thống Cấp độ 3) hoặc ngay khi có sự thay đổi, nâng cấp, mở rộng kiến trúc.

3. Truy cập mạng của máy chủ:

a) Mọi kết nối, truy cập máy chủ phải được kiểm soát bởi hệ thống tường lửa (Firewall) của hệ thống.

b) Chỉ mở cổng quản trị hệ thống từ vùng mạng quản trị (Management Zone) hoặc vùng mạng nội bộ (LAN) được quy hoạch riêng; cấm quản trị trực tiếp từ Internet.

c) Không cho phép hoặc giới hạn truy cập từ các máy chủ bên trong hệ thống ra các mạng bên ngoài (Internet) chỉ với những cổng/dịch vụ thực sự cần thiết theo yêu cầu nghiệp vụ.

4. Truy cập và quản trị máy chủ, ứng dụng:

a) Phải thay đổi hoặc vô hiệu hóa các tài khoản, mật khẩu mặc định của hệ thống ngay khi đưa hệ điều hành, phần mềm vào sử dụng. Định kỳ yêu cầu thay đổi mật khẩu quản trị tối thiểu 03 tháng/lần và thiết lập quy tắc độ phức tạp của mật khẩu.

b) Chỉ cấp quyền quản lý máy chủ và ứng dụng cho cán bộ quản trị theo chức năng, nhiệm vụ được giao (nguyên tắc quyền tối thiểu); thu hồi quyền ngay khi cán bộ thay đổi công việc hoặc nghỉ việc.

c) Truy cập quản trị máy chủ và ứng dụng phải thông qua các giao thức mạng an toàn, có mã hóa (như SSL/TLS, SSH, VPN).

d) Truy cập quản trị máy chủ và ứng dụng từ bên ngoài mạng cơ quan phải thông qua kênh kết nối mạng riêng ảo (VPN).

5. Cập nhật, sao lưu dự phòng và khôi phục sự cố:

a) Định kỳ hoặc khi có thay đổi cấu hình, nâng cấp ứng dụng, phải thực hiện sao lưu dự phòng: Tập cấu hình hệ thống, bản dự phòng hệ điều hành, mã nguồn ứng dụng và cơ sở dữ liệu trên phương tiện lưu trữ độc lập (offline backup hoặc hệ thống backup chuyên dụng).

b) Dữ liệu lưu trữ dự phòng quan trọng phải được mã hóa và có mã kiểm tra tính nguyên vẹn dữ liệu.

c) Dữ liệu sao lưu phải được quản lý theo phiên bản, có phân quyền truy cập nghiêm ngặt và định kỳ kiểm tra khả năng khôi phục (restore test) từ bản sao lưu.

6. Cấu hình tối ưu và tăng cường bảo mật (cứng hóa - Hardening): Các máy chủ trước khi đưa vào vận hành khai thác phải được thực hiện cứng hóa, bao gồm:

a) Sử dụng hệ điều hành bảo đảm an toàn thông tin, đã được cập nhật các bản vá mới nhất.

b) Loại bỏ hoặc tắt tất cả các dịch vụ, giao thức, cổng mạng không cần thiết cho hoạt động nghiệp vụ.

c) Sử dụng các phiên bản phần mềm an toàn, không sử dụng phần mềm đã bị ngừng hỗ trợ (End of Life).

d) Thiết lập kiểm soát truy cập ở cấp độ người dùng cho mỗi dịch vụ; phân quyền giới hạn tài nguyên hệ thống (file, thư mục) chặt chẽ.

7. Cài đặt, gỡ bỏ hệ điều hành, dịch vụ, phần mềm trên hệ thống máy chủ và ứng dụng

a) Mọi yêu cầu cài đặt mới, nâng cấp hoặc gỡ bỏ hệ điều hành, dịch vụ, phần mềm trên máy chủ phải được lập kế hoạch, đánh giá rủi ro và được sự phê duyệt bằng văn bản (hoặc qua hệ thống quản lý yêu cầu - Ticketing) của bộ phận/người có thẩm quyền. Người dùng không được tự ý can thiệp (thay đổi, gỡ bỏ, cài đặt) vào hệ thống.

b) Các phần mềm, dịch vụ mới phải được cài đặt thử nghiệm, rà quét mã độc/lỗ hổng trên môi trường thử nghiệm (Test/Staging) trước khi triển khai lên môi trường vận hành thực tế (Production).

c) Khi gỡ bỏ các dịch vụ, phần mềm không còn nhu cầu sử dụng, quản trị viên phải thực hiện xóa bỏ triệt để các tệp tin cấu hình, tài khoản người dùng đi kèm và đóng các cổng kết nối tương ứng trên tường lửa để tránh tạo ra lỗ hổng bảo mật.

d) Toàn bộ quá trình cài đặt, gỡ bỏ phải được ghi nhận vào nhật ký quản trị sự thay đổi (Change Log).

8. Kết nối và gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống

a) Khi kết nối máy chủ mới vào hệ thống: Máy chủ (vật lý hoặc máy chủ ảo) chỉ được phép kết nối vào phân vùng mạng vận hành sau khi đã hoàn tất quy trình thử nghiệm, nghiệm thu, thực hiện cấu hình tăng cường bảo mật (cứng hóa tại Khoản 6 Điều này) và được cấp thẩm quyền phê duyệt.

b) Khi gỡ bỏ/chuyển giao máy chủ khỏi hệ thống:

- Phải thực hiện sao lưu toàn bộ dữ liệu quan trọng và nhật ký hệ thống trước khi gỡ bỏ.

- Phải sử dụng các biện pháp chuyên dụng để xóa sạch thông tin, dữ liệu trên máy chủ (Secure Wipe) bảo đảm dữ liệu không thể khôi phục khi chuyển giao thiết bị cho bên thứ ba hoặc thay đổi mục đích sử dụng.

- Phải thu hồi ngay lập tức địa chỉ IP, dọn dẹp các chính sách truy cập (Rules) trên tường lửa, loại bỏ máy chủ khỏi hệ thống giám sát tập trung và cập nhật lại hồ sơ thiết kế, danh mục tài sản của hệ thống.

Điều 15. Quản lý lỗ hổng bảo mật và Nhật ký an ninh mạng

1. Lỗ hổng bảo mật: Rà soát và cập nhật quy trình đánh giá, xử lý lỗ hổng bảo mật tối thiểu 01 lần/năm hoặc khi xảy ra thay đổi lớn.

2. Nhật ký (Log): Đảm bảo duy trì không gian lưu trữ nhật ký tối thiểu 12 tháng để tránh thất thoát dữ liệu. Định kỳ thực hiện rà soát nhật ký an ninh mạng tối thiểu 01 lần/tuần.

Điều 16. Quản lý an toàn dữ liệu

1. Quy định dự phòng và khôi phục dữ liệu:

a) Định kỳ hàng tuần phải sao lưu, dự phòng cơ sở dữ liệu và dữ liệu nghiệp vụ (nếu có) trên thiết bị hoặc hệ thống độc lập.

b) Dữ liệu lưu trữ phải được mã hóa thích hợp theo các chuẩn quốc gia hoặc quốc tế đã được công nhận để bảo vệ thông tin cùng mã kiểm tra tính nguyên vẹn.

c) Dữ liệu lưu trữ phải được quản lý theo phiên bản và có quản lý truy cập.

2. Định kỳ hàng tháng hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

3. Sao lưu dự phòng và khôi phục dữ liệu

a) Lập danh sách các dữ liệu, phần mềm cần được sao lưu, có phân loại theo thời gian lưu trữ, thời gian sao lưu, phương pháp sao lưu và thời gian kiểm tra phục hồi hệ thống từ dữ liệu sao lưu.

b) Đơn vị vận hành xây dựng tài liệu, quy trình hướng dẫn sao lưu/phục hồi dữ liệu của hệ thống: tần suất sao lưu dự phòng, phương tiện lưu trữ, thời gian lưu trữ; nơi lưu trữ, phương thức lưu trữ và phương thức lấy dữ liệu ra khỏi phương tiện lưu trữ....

4. Dữ liệu cấp độ mật phải được mã hoá bằng giải pháp bảo mật của Ban Cơ yếu Chính phủ.

Điều 17. Quản lý an toàn thiết bị đầu cuối

1. Quản lý, vận hành hoạt động bình thường cho thiết bị đầu cuối:

a) Toàn bộ thiết bị đầu cuối tham gia vào hệ thống (máy trạm người dùng, máy trạm quản trị, thiết bị đặc thù) phải được lập hồ sơ quản lý thông tin tài sản bao gồm: tên thiết bị, chủng loại, hệ điều hành, địa chỉ MAC, địa chỉ IP và thông tin người sử dụng/quản lý. Hồ sơ này phải được cập nhật ngay khi có sự thay đổi.

b) Thiết bị đầu cuối phải được cài đặt phần mềm phòng chống mã độc có bản quyền, có tính năng quản lý tập trung và tự động cập nhật cơ sở dữ liệu mẫu nhận dạng. Người dùng tuyệt đối không được tự ý vô hiệu hóa hoặc gỡ bỏ phần mềm bảo mật này.

c) Hệ điều hành và các phần mềm cài đặt trên thiết bị đầu cuối phải được cấu hình cập nhật bản vá lỗi định kỳ để khắc phục các lỗ hổng bảo mật. d) Các chính sách bảo mật (Group Policy) phải được thiết lập để khóa tự động màn hình khi thiết bị không được sử dụng trong một khoảng thời gian nhất định và kiểm soát chặt chẽ việc sử dụng các cổng kết nối ngoại vi (như USB, ổ cứng di động) nhằm ngăn ngừa lây nhiễm mã độc và rò rỉ dữ liệu.

2. Kết nối, truy cập và sử dụng thiết bị đầu cuối từ xa:

a) Cán bộ, nhân viên khi sử dụng thiết bị đầu cuối để truy cập, quản trị hoặc làm việc từ xa vào mạng nội bộ của cơ quan phải thông qua kênh kết nối mạng riêng ảo (VPN) và sử dụng các giao thức mạng an toàn có mã hóa.

b) Việc kết nối từ xa phải được thiết lập cơ chế xác thực chặt chẽ (khuyến khích áp dụng xác thực đa nhân tố - MFA) và chỉ được cấp quyền truy cập tối thiểu đủ để thực hiện nhiệm vụ (Least Privilege).

c) Nghiêm cấm lưu trữ các tài liệu, cơ sở dữ liệu nhạy cảm của hệ thống trên thiết bị đầu cuối cá nhân (BYOD) mang về nhà, trừ trường hợp thiết bị đó đã được mã hóa ổ cứng và được sự phê duyệt bằng văn bản của lãnh đạo cơ quan.

3. Cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống:

a) Việc kết nối một thiết bị đầu cuối mới vào hệ thống mạng nội bộ phải được phê duyệt bởi người có thẩm quyền. Thiết bị phải được bộ phận chuyên trách công nghệ thông tin kiểm tra (cài đặt phần mềm diệt virus, cập nhật hệ điều hành) và đăng ký thông tin nhận diện (MAC/IP) vào hệ thống Quản lý truy cập mạng (nếu có) trước khi được hòa mạng.

b) Khi một thiết bị đầu cuối bị hỏng, thay đổi mục đích sử dụng hoặc người sử dụng chuyển công tác/ngỉ việc, bộ phận quản trị phải ngay lập tức thực hiện quy trình gỡ bỏ: thu hồi tài khoản, dọn dẹp các quyền truy cập mạng, vô hiệu hóa địa chỉ IP và cập nhật lại danh sách tài sản.

c) Trước khi mang thiết bị đầu cuối đi bảo hành, thanh lý hoặc chuyển giao cho cá nhân/tổ chức khác, bộ phận kỹ thuật phải sao lưu dữ liệu công việc (nếu cần) và sử dụng các công cụ chuyên dụng để xóa sạch toàn bộ dữ liệu trên ổ cứng (Secure Wipe) đảm bảo không thể khôi phục lại dưới mọi hình thức.

Điều 18. Quản lý sự cố an toàn thông tin

1. Phân nhóm sự cố an toàn thông tin mạng theo quy định tại Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ ngày 16/3/2017 quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia (Quyết định 05); Xây dựng phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng, ứng phó sự cố an toàn thông tin mạng.

2. Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng: Sở Công Thương cùng các đơn vị vận hành xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13, 14 Quyết định số 05/2017/QĐ-TTg.

3. Kế hoạch ứng phó sự cố an toàn thông tin mạng: Sở Công Thương cùng các đơn vị vận hành xây dựng và triển khai kế hoạch ứng phó sự cố an toàn thông tin theo quy định tại Điều 16 Quyết định số 05/2017/QĐ-TTg.

4. Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin.

a. Sở Công Thương cùng các đơn vị vận hành điều động nhân lực có kinh nghiệm thực hiện giám sát, phát hiện và cảnh báo sự cố an toàn thông tin, phối hợp với các đơn vị chuyên trách về ATTT đưa ra cảnh báo sớm về nguy cơ mất ATTT trong hệ thống.

b. Đối với người dùng: Thông tin, báo cáo kịp thời cho cán bộ chuyên trách về ATTT của đơn vị khi phát hiện các sự cố gây mất ATTT trong quá trình tham gia vào hệ thống thông tin của đơn vị; Phối hợp tích cực trong suốt quá trình giải quyết và khắc phục sự cố.

5. Quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng: Sở Công Thương cùng các đơn vị vận hành xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13, 14 Quyết định số 05/2017/QĐ-TTg.

6. Công chức phụ trách về Thông tin quyết định toàn diện về mặt kỹ thuật đối với các cơ quan trong quá trình khắc phục sự cố về ATTT; hỗ trợ, phối hợp và hướng dẫn các cơ quan khắc phục sự cố mất ATTT; yêu cầu ngưng hoạt động một phần hoặc toàn bộ các hệ thống thông tin của các cơ quan nhằm phục vụ công tác khắc phục sự cố về ATTT; phối hợp với đơn vị chức năng trong điều tra các nguyên nhân gây ra sự cố mất an toàn thông tin theo chỉ đạo của lãnh đạo.

7. Phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin; yêu cầu bên cung cấp, hỗ trợ cung cấp quy trình xử lý sự cố cho các dịch vụ do bên cung cấp, hỗ trợ cung cấp liên quan đến hệ thống.

8. Định kỳ tổ chức diễn tập phương án xử lý sự cố an toàn thông tin hoặc theo chỉ đạo của lãnh đạo.

Điều 19. Quản lý an toàn người sử dụng đầu cuối

1. Quản lý truy cập, sử dụng tài nguyên nội bộ

a) Bảo đảm an toàn thông tin, an ninh mạng, bảo vệ dữ liệu cá nhân theo thẩm quyền được giao.

b) Chủ động báo cáo kết quả tình trạng hoạt động, sự cố khi sử dụng thiết bị không đảm bảo an ninh, an toàn.

c) Có trách nhiệm quản lý tài khoản, thiết bị truy cập hệ thống thông tin được quản lý và chịu trách nhiệm nêu vi phạm theo các nội dung tại Quy định này.

d) Thực hiện đúng quy định hiện hành của Nhà nước về quản lý, sử dụng thiết bị, phần mềm.

đ) Bảo quản, giữ gìn, bảo đảm sử dụng lâu bền, tiết kiệm, thiết thực, hiệu quả.

e) Phối hợp với đơn vị chuyên trách về công nghệ thông tin của đơn vị trong việc bảo trì thiết bị và phần mềm tin học, sao lưu dữ liệu (nếu cần thiết), xóa dữ liệu trong máy tính trước khi bàn giao, điều chuyển hoặc thanh lý.

f) Bàn giao các thiết bị tin học, thiết bị lưu trữ điện tử khi không còn công tác tại cơ quan. Giao nộp kịp thời các thiết bị lưu trữ điện tử cũ, hỏng, không sử dụng được và không được phép tự hủy, hoặc để thất thoát ra bên ngoài cơ quan.

2. Quản lý truy cập mạng và tài nguyên trên Internet

a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao.

b) Người sử dụng chỉ được truy cập các tài nguyên mạng, hệ thống thông tin và dịch vụ Internet phù hợp với chức năng, nhiệm vụ được giao; không được tự ý truy cập trái phép vào các hệ thống, dịch vụ không được cấp quyền.

c) Áp dụng các biện pháp kỹ thuật để kiểm soát, giám sát và ngăn chặn truy cập tới các trang thông tin điện tử, dịch vụ Internet có nguy cơ mất an toàn thông tin, chứa mã độc hoặc nội dung không phù hợp.

d) Nghiêm cấm việc sử dụng mạng của cơ quan, đơn vị để: Truy cập, phát tán nội dung vi phạm pháp luật; phát tán thư rác, mã độc, phần mềm không rõ nguồn gốc; thực hiện các hành vi gây mất an toàn thông tin mạng hoặc ảnh hưởng đến hoạt động của cơ quan, đơn vị.

đ) Việc tải xuống, cài đặt và sử dụng phần mềm từ Internet phải được kiểm soát; chỉ được phép cài đặt các phần mềm phục vụ công việc, có nguồn gốc rõ ràng và được phê duyệt theo quy định.

e) Kết nối từ xa vào hệ thống thông tin của đơn vị phải thông qua các giải pháp bảo mật theo quy định (như VPN, xác thực đa yếu tố hoặc các biện pháp tương đương).

f) Thực hiện phân tách và kiểm soát truy cập giữa các vùng mạng (mạng nội bộ, mạng quản trị, mạng Internet, mạng khách) nhằm hạn chế nguy cơ tấn công và lây lan mã độc.

g) Hoạt động truy cập mạng và sử dụng tài nguyên Internet phải được ghi nhận, lưu trữ nhật ký để phục vụ công tác kiểm tra, giám sát và xử lý sự cố khi cần thiết.

h) Định kỳ hoặc khi cần thiết, thực hiện rà soát, đánh giá việc sử dụng mạng và tài nguyên Internet nhằm phát hiện nguy cơ, hành vi vi phạm và có biện pháp xử lý kịp thời.

i) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách công nghệ thông tin của cơ quan, đơn vị để kịp thời ngăn chặn và xử lý.

Điều 20. Quản lý phòng chống phần mềm độc hại

1. Cài đặt, cập nhật và sử dụng phần mềm phòng chống mã độc:

a) Tất cả các máy chủ, máy tính (máy trạm) và thiết bị di động tham gia vào hệ thống phải được cài đặt phần mềm phòng chống mã độc đáp ứng yêu cầu tại Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ.

b) Phần mềm phòng chống mã độc phải được thiết lập tự động cập nhật cơ sở dữ liệu mẫu nhận dạng và chế độ bảo vệ theo thời gian thực. Thường xuyên thực hiện dò quét, kiểm tra phần mềm độc hại trên máy tính, máy chủ và thiết bị di động.

2. Quản lý cài đặt phần mềm và truy cập mạng:

a) Người sử dụng không được tự ý cài đặt, sử dụng các phần mềm lạ, không rõ nguồn gốc trên máy tính và thiết bị di động của đơn vị khi chưa được bộ phận chuyên trách công nghệ thông tin kiểm tra và cho phép.

b) Người sử dụng phải tuân thủ nghiêm các quy định an toàn khi truy cập các trang thông tin trên mạng Internet; nghiêm cấm truy cập vào các trang web không an toàn, có nguy cơ phát tán mã độc.

3. Kiểm soát gửi nhận tập tin và phương tiện lưu trữ di động: Tất cả các tập tin, phần mềm ứng dụng khi gửi và nhận qua môi trường mạng (email, các hệ thống trao đổi thông tin) hoặc sao chép từ các phương tiện lưu trữ di động (USB, thẻ nhớ, ổ cứng ngoài) bắt buộc phải được quét kiểm tra mã độc trước khi sao chép, mở, cài đặt hoặc sử dụng.

4. Dò quét định kỳ và xử lý sự cố mã độc:

a) Định kỳ hàng tháng (có thể điều chỉnh thành hàng tuần tùy quy mô đơn vị) thực hiện kiểm tra và dò quét phần mềm độc hại toàn diện trên toàn bộ hệ thống.

b) Thực hiện kiểm tra và xử lý ngay lập tức khi phát hiện dấu hiệu hoặc có cảnh báo về sự xuất hiện của phần mềm độc hại trên hệ thống.

c) Khi phát hiện bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm mã độc trên thiết bị (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, bị đổi tên tệp tin, mất dữ liệu,...), người sử dụng phải lập tức ngắt kết nối mạng của thiết bị và báo trực tiếp cho bộ phận có trách nhiệm của đơn vị để tiến hành bóc gỡ, xử lý.

Điều 21. Quản lý giám sát an toàn hệ thống thông tin

1. Triển khai, quản lý và vận hành hệ thống giám sát an toàn thông tin tập trung bảo đảm hoạt động thường xuyên, liên tục, đáp ứng yêu cầu tại khoản 1 Điều 5 Thông tư số 31/2017/TT-BTTTT.

2. Đối tượng giám sát bao gồm các thiết bị hệ thống, máy chủ, ứng dụng, dịch vụ và các thành phần khác trong hệ thống thông tin (nếu có). Thông tin giám sát và danh mục các đối tượng giám sát phải đáp ứng yêu cầu tại khoản 2 Điều 5 Thông tư số 31/2017/TT-BTTTT.

3. Thực hiện kết nối, thu thập và gửi nhật ký hệ thống từ các đối tượng giám sát về hệ thống giám sát tập trung; bảo đảm việc lưu trữ, bảo vệ và quản lý an toàn thông tin giám sát, nhật ký hệ thống theo quy định.

4. Thực hiện quản lý truy cập, phân quyền và quản trị hệ thống giám sát; bảo đảm đồng bộ thời gian giữa hệ thống giám sát và các thiết bị, hệ thống được giám sát.

5. Thực hiện theo dõi, giám sát, phát hiện và cảnh báo kịp thời các sự cố, dấu hiệu mất an toàn thông tin trên hệ thống thông tin; triển khai các nhiệm vụ giám sát theo quy định tại khoản 3 Điều 5 Thông tư số 31/2017/TT-BTTTT.

Điều 22. Quản lý điểm yếu an toàn thông tin

Đơn vị vận hành có trách nhiệm:

1. Quản lý thông tin điểm yếu an toàn thông tin đối với từng thành phần có trong hệ thống (hệ điều hành, máy chủ, ứng dụng, dịch vụ...); phân loại mức độ nguy hiểm của điểm yếu; xây dựng phương án và quy trình xử lý đối với từng mức độ nguy hiểm của điểm yếu.

2. Báo cáo lãnh đạo/cán bộ quản lý ngay khi phát hiện điểm yếu an toàn thông tin ở mức độ nghiêm trọng. Thực hiện cảnh báo và xử lý điểm yếu an toàn thông tin theo chỉ đạo. Việc xử lý điểm yếu an toàn thông tin phải bảo đảm không làm ảnh hưởng/gián đoạn hoạt động của hệ thống.

3. Xây dựng phương án xử lý tạm thời đối với trường hợp điểm yếu an toàn thông tin chưa được khắc phục và phương án khôi phục hệ thống trong trường hợp xử lý điểm yếu thất bại.

4. Có trách nhiệm phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu an toàn thông tin đối với các điểm yếu khi cần thiết.

5. Kiểm tra, đánh giá và xử lý điểm yếu an toàn thông tin cho thiết bị hệ thống, máy chủ, dịch vụ trước khi đưa vào sử dụng.

6. Định kỳ 01 năm kiểm tra, đánh giá điểm yếu an toàn thông tin cho toàn bộ hệ thống thông tin; Thực hiện quy trình kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin khi có thông tin hoặc nhận được cảnh báo về điểm yếu an toàn thông tin đối với thành phần cụ thể trong hệ thống.

Điều 23. Quản lý rủi ro an toàn thông tin mạng

1. Nguyên tắc chung: Việc quản lý rủi ro an toàn thông tin mạng phải được thực hiện thường xuyên, liên tục trong suốt vòng đời của hệ thống thông tin nhằm phát hiện, kiểm soát và giảm thiểu các nguy cơ gây mất an toàn thông tin; bảo đảm rủi ro được duy trì trong ngưỡng chấp nhận được của đơn vị.

2. Nội dung quản lý rủi ro an toàn thông tin mạng

a) Xác định rủi ro:

- Xác định tài sản thông tin (dữ liệu, hệ thống, ứng dụng, hạ tầng kỹ thuật).
- Xác định các mối đe dọa, lỗ hổng, điểm yếu có thể ảnh hưởng đến tài sản thông tin.

- Xác định các kịch bản rủi ro có thể xảy ra.

b) Phân tích rủi ro:

- Phân tích khả năng xảy ra của từng kịch bản rủi ro.
- Phân tích mức độ ảnh hưởng đối với hoạt động của đơn vị khi rủi ro xảy ra.
- Xác định mức độ rủi ro dựa trên tiêu chí kết hợp giữa khả năng xảy ra và mức độ ảnh hưởng.

c) Đánh giá rủi ro

- Phân loại rủi ro theo các mức: cao, trung bình, thấp hoặc theo tiêu chí do đơn vị quy định.
- So sánh mức độ rủi ro với ngưỡng chấp nhận rủi ro của đơn vị để làm cơ sở xử lý.

d) Xử lý rủi ro

Định kỳ 06 tháng phải tiến hành đánh giá và cải thiện hiệu quả của các biện pháp kiểm soát được sử dụng để giảm thiểu rủi ro trong đó lựa chọn và áp dụng một hoặc nhiều biện pháp xử lý rủi ro, bao gồm:

- Giảm thiểu rủi ro thông qua việc triển khai các biện pháp kỹ thuật và quản lý;
- Tránh rủi ro bằng cách thay đổi, dừng hoặc không triển khai hoạt động có rủi ro;
- Chuyển giao rủi ro thông qua thuê dịch vụ hoặc các hình thức phù hợp;
- Chấp nhận rủi ro khi rủi ro nằm trong ngưỡng chấp nhận.
- Xây dựng kế hoạch xử lý rủi ro, trong đó xác định rõ biện pháp, lộ trình, nguồn lực và trách nhiệm thực hiện.

đ) Chấp nhận rủi ro

- Việc chấp nhận rủi ro phải được xem xét, phê duyệt bởi người có thẩm quyền theo quy định của đơn vị.
- Các rủi ro được chấp nhận phải được lập thành hồ sơ, nêu rõ lý do chấp nhận và thời hạn xem xét lại.

e) Theo dõi và rà soát rủi ro

- Thực hiện theo dõi, giám sát tình trạng rủi ro định kỳ hoặc khi có thay đổi đối với hệ thống thông tin.
- Rà soát, cập nhật đánh giá rủi ro khi xuất hiện mối đe dọa mới, lỗ hổng mới hoặc thay đổi về công nghệ, quy trình.
- Đánh giá lại hiệu quả các biện pháp xử lý rủi ro đã triển khai.

g) Hồ sơ và báo cáo rủi ro

- Thiết lập và duy trì danh mục rủi ro an toàn thông tin.
- Lưu trữ đầy đủ kết quả đánh giá, xử lý, chấp nhận rủi ro.
- Thực hiện chế độ báo cáo định kỳ hoặc đột xuất về tình hình rủi ro an toàn thông tin theo quy định.

3. Hình thức thực hiện quản lý rủi ro

- Thực hiện định kỳ theo kế hoạch hằng năm hoặc theo quy định của pháp luật.
- Thực hiện đột xuất khi có yêu cầu của cấp có thẩm quyền hoặc khi phát sinh sự cố, nguy cơ mất an toàn thông tin.

4. Trách nhiệm thực hiện

- Đơn vị chuyên trách an toàn thông tin: chủ trì tổ chức đánh giá và quản lý rủi ro.
- Đơn vị vận hành, quản trị hệ thống thông tin: phối hợp cung cấp thông tin, triển khai biện pháp xử lý rủi ro.
- Lãnh đạo đơn vị: xem xét, phê duyệt việc xử lý và chấp nhận rủi ro.
- Các cá nhân, bộ phận liên quan: có trách nhiệm tuân thủ các biện pháp kiểm soát rủi ro đã được ban hành.

Điều 24. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

Quy định, quy trình về Kết thúc vận hành, khai thác, thanh lý, hủy bỏ bao gồm các nội dung sau:

1. Thiết bị công nghệ thông tin có chứa dữ liệu (máy tính, thiết bị lưu trữ, ...) khi bị hỏng phải được cán bộ vận hành kiểm tra, sửa chữa, khắc phục. Phải có biện pháp kiểm tra, giám sát đảm bảo không để lọt lộ thông tin hay lây nhiễm mã độc đối với máy tính mang ra bên ngoài sửa chữa, bảo hành.

2. Trước khi tiến hành thanh lý/loại bỏ thiết bị công nghệ thông tin cũ, phải áp dụng các biện pháp kỹ thuật xóa bỏ hoàn toàn dữ liệu người dùng đã tạo ra, đảm bảo không thể phục hồi.

3. Các phương tiện và thiết bị công nghệ thông tin: Máy tính cá nhân (PC), máy tính xách tay, máy chủ, các thiết bị mạng, phương tiện lưu trữ như CD/DVD, thẻ nhớ, ổ cứng phải xóa sạch dữ liệu khi chuyển giao hoặc thay đổi mục đích sử dụng.

Điều 25. Bảo vệ bí mật nhà nước trong hoạt động ứng dụng công nghệ thông tin

1. Quy định về soạn thảo, in ấn, phát hành và sao chụp tài liệu mật:

a) Dữ liệu cấp độ mật phải được mã hoá bằng giải pháp bảo mật của Ban Cơ yếu Chính phủ.

b) Không được soạn thảo, lưu giữ, chuyển giao, đăng tải, phát tán thông tin,

tài liệu có chứa nội dung bí mật nhà nước trên máy tính hoặc thiết bị khác đã kết nối hoặc đang kết nối với mạng Internet, mạng máy tính, mạng viễn thông, trừ trường hợp lưu giữ bí mật nhà nước theo quy định của pháp luật về cơ yếu.

c) Không được in, sao chụp tài liệu bí mật nhà nước trên các thiết bị kết nối mạng internet.

d) Phải bố trí ít nhất 01 máy vi tính độc lập riêng, không kết nối mạng nội bộ và mạng Internet dùng để quản lý, soạn thảo, lưu trữ các tài liệu mật của nhà nước theo quy định.

2. Khi sửa chữa, khắc phục các sự cố của máy tính dùng soạn thảo văn bản mật, các phòng, đơn vị phải báo cáo cho người có thẩm quyền. Không được cho phép các tổ chức, cá nhân không có trách nhiệm trực tiếp sửa chữa, xử lý, khắc phục sự cố.

3. Trước khi thanh lý các máy tính trong các cơ quan nhà nước phải dùng các biện pháp kỹ thuật xóa bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính.

4. Nghiêm cấm chuyển đổi mục đích sử dụng máy tính để soạn thảo, lưu trữ thông tin mật có nội dung bí mật nhà nước sang máy tính có kết nối Internet và ngược lại mà chưa làm sạch và thực hiện giải pháp huỷ dữ liệu triệt để.

Chương IV **TỔ CHỨC THỰC HIỆN**

Điều 26. Bộ phận chuyên trách về an toàn thông tin

1. Giao công chức phụ trách về công nghệ thông tin, chuyển đổi số là bộ phận chuyên trách về an toàn thông tin, có trách nhiệm bảo đảm an toàn thông tin cho hệ thống thông tin. Văn phòng Sở là bộ phận vận hành Hệ thống thông tin.

2. Văn phòng Sở là đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin; Có trách nhiệm phổ biến hướng dẫn triển khai Quy chế này và các quy định về an toàn thông tin có liên quan.

3. Văn phòng Sở phối hợp với các phòng, đơn vị thuộc Sở tham mưu thực hiện chế độ báo cáo định kỳ theo quy định của pháp luật, báo cáo đột xuất theo yêu cầu của cấp trên.

Điều 27. Xây dựng và công bố

Quy chế này được Văn phòng Sở trình người đứng đầu đơn vị vận hành duyệt, ký trước khi công bố áp dụng.

Điều 28. Trách nhiệm của các bộ phận, tổ chức, cá nhân

a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về an toàn thông tin. Chịu trách nhiệm bảo đảm ATTT mạng, bảo vệ BMNN trong phạm vi trách nhiệm và quyền hạn được giao;

b) Mỗi cán bộ, công chức, viên chức và người lao động phải có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng.

c) Khi phát hiện nguy cơ hoặc sự cố mất ATTT phải báo cáo ngay với cấp trên và bộ phận kiêm nhiệm hoặc Trung tâm Truyền thông, Dữ liệu và Công nghệ số để kịp thời ngăn chặn và xử lý;

d) Tham gia các chương trình đào tạo, hội nghị về ATTT mạng được tỉnh hoặc đơn vị có liên quan tổ chức.

Điều 29. Khen thưởng và xử lý vi phạm

1. Xem xét, khen thưởng cho các cá nhân, phòng, đơn vị có nhiều thành tích trong công tác bảo đảm an toàn thông tin mạng trong quản lý, vận hành, khai thác Hệ thống thông tin của Sở.

2. Tổ chức, cá nhân có hành vi vi phạm quy chế này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý theo quy định hiện hành.

Điều 30. Tổ chức triển khai Quy chế

1. Quy định trong Quy chế này có hiệu lực thi hành kể từ ngày ký ban hành.

2. Định kỳ 02 năm hoặc khi có thay đổi Quy chế bảo đảm an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung.

3. Trong quá trình thực hiện quy chế, nếu có vấn đề vướng mắc, phát sinh, cán bộ, công chức phản ánh kịp thời về Văn phòng Sở để tổng hợp báo cáo Lãnh đạo Sở Công Thương xem xét điều chỉnh, bổ sung./.

SỞ CÔNG THƯƠNG TỈNH HƯNG YÊN