BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 12 /2022/TT-BTTTT	*Hà Nội, ngày 12 tháng 8 năm 2022*

THÔNG TƯ
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 bảo đảm an toàn hệ thống thông tin theo cấp độ

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 48/2022/NĐ-CP ngày 26 tháng 7 năm 2022 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Thông tin và Truyền thông;

Theo đề nghị của Cục trưởng Cục An toàn thông tin;

Bộ trưởng Bộ Thông tin và Truyền thông ban hành Thông tư quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ.

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Thông tư này quy định chi tiết và hướng dẫn bảo đảm an toàn hệ thống thông tin theo cấp độ, bao gồm: xác định hệ thống thông tin và thuyết minh cấp độ an toàn hệ thống thông tin; yêu cầu bảo đảm an toàn hệ thống thông tin theo cấp độ; kiểm tra, đánh giá an toàn thông tin; chế độ báo cáo.

Điều 2. Đối tượng áp dụng

Đối tượng áp dụng Thông tư này được thực hiện theo quy định tại Điều 2 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 (sau đây gọi tắt là Nghị định 85/2016/NĐ-CP).

Điều 3. Giải thích từ ngữ

Trong Thông tư này, các từ ngữ dưới đây được hiểu như sau:

1. *Dự phòng nóng* là khả năng thay thế chức năng của thiết bị khi xảy ra sự cố mà không làm gián đoạn hoạt động của hệ thống.

2. *Thiết bị mạng chính hoặc quan trọng* là các thiết bị trong hệ thống khi bị ngừng hoạt động mà không có kế hoạch trước sẽ làm gián đoạn hoạt động của toàn bộ hệ thống thông tin. Thành phần thiết bị mạng chính được xác định theo cấp độ của hệ thống thông tin, bao gồm tối thiểu: thiết bị chuyển mạch trung tâm hoặc tương đương, thiết bị tường lửa trung tâm, tường lửa ứng dụng web, hệ thống lưu trữ tập trung, tường lửa cơ sở dữ liệu.

Điều 4. Chủ quản hệ thống thông tin

1. Đối với các Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương, chủ quản hệ thống thông tin là một trong các trường hợp sau:

a) Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;

b) Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương;

c) Cấp có thẩm quyền quyết định đầu tư dự án xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin. Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương quyết định chủ quản hệ thống thông tin theo quy định của khoản này, bảo đảm cơ quan, tổ chức được giao chủ quản hệ thống thông tin có đủ năng lực để thực thi đầy đủ các quy định tại Điều 20 Nghị định 85/2016/NĐ-CP.

2. Đối với doanh nghiệp và tổ chức khác (không phải Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương), chủ quản hệ thống thông tin là cấp có thẩm quyền quyết định đầu tư xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin.

3. Trong trường hợp cần thiết, chủ quản hệ thống thông tin ủy quyền cho một tổ chức trực thuộc có đủ năng lực để thay mặt thực hiện trách nhiệm của chủ quản hệ thống thông tin quy định tại khoản 2 Điều 20 Nghị định 85/2016/NĐ-CP.

Việc ủy quyền trách nhiệm chủ quản hệ thống thông tin phải được thực hiện bằng văn bản, trong đó nêu rõ phạm vi của hệ thống, trách nhiệm của tổ chức được ủy quyền và thời hạn ủy quyền.

Điều 5. Đơn vị vận hành hệ thống thông tin

1. Đơn vị vận hành hệ thống thông tin là cơ quan, tổ chức được chủ quản hệ thống thông tin giao nhiệm vụ vận hành hệ thống thông tin.

2. Trong trường hợp hệ thống thông tin gồm nhiều hệ thống thành phần hoặc phân tán, có nhiều hơn một đơn vị vận hành hệ thống thông tin, chủ quản hệ thống thông tin có trách nhiệm chỉ định một đơn vị chủ trì thực hiện quyền và nghĩa vụ của đơn vị vận hành hệ thống thông tin theo quy định của pháp luật.

3. Trong trường hợp thuê dịch vụ công nghệ thông tin, đơn vị vận hành hệ thống thông tin được xác định như sau:

a) Trường hợp chưa xác định được đơn vị cung cấp dịch vụ theo quy định của pháp luật, đơn vị chủ trì thuê dịch vụ đóng vai trò là đơn vị vận hành;

b) Trường hợp đã xác định được đơn vị cung cấp dịch vụ theo quy định của pháp luật thì đơn vị vận hành là đơn vị cung cấp dịch vụ;

c) Trường hợp hết thời hạn cung cấp dịch vụ, nếu hệ thống thông tin được thiết lập qua hình thức thuê dịch vụ vẫn tiếp tục duy trì hoạt động, đơn vị vận hành được xác định là đơn vị chủ trì thuê dịch vụ.

Điều 6. Thẩm định Hồ sơ đề xuất cấp độ trong trường hợp đơn vị chuyên trách về an toàn thông tin đồng thời được chủ quản hệ thống thông tin giao quản lý, vận hành hệ thống thông tin

Trường hợp đơn vị chuyên trách về an toàn thông tin, đồng thời được chủ quản hệ thống thông tin giao quản lý, vận hành hệ thống thông tin, việc tổ chức thẩm định Hồ sơ đề xuất cấp độ được thực hiện theo một trong các phương án sau đây:

1. Đơn vị chuyên trách về an toàn thông tin trình chủ quản hệ thống thông tin giao một đơn vị trực thuộc có đủ năng lực chủ trì, tổ chức thẩm định.

2. Đơn vị chuyên trách về an toàn thông tin trình chủ quản hệ thống thông tin thành lập Hội đồng thẩm định độc lập thực hiện nhiệm vụ thẩm định Hồ sơ đề xuất cấp độ.

Chương II
XÁC ĐỊNH HỆ THỐNG THÔNG TIN VÀ THUYẾT MINH CẤP ĐỘ AN TOÀN HỆ THỐNG THÔNG TIN

Điều 7. Xác định hệ thống thông tin

1. Việc xác định hệ thống thông tin để xác định cấp độ căn cứ trên nguyên tắc được quy định tại khoản 1 Điều 5 Nghị định 85/2016/NĐ-CP.

2. Hệ thống thông tin phục vụ hoạt động nội bộ là hệ thống chỉ phục vụ hoạt động quản trị, vận hành nội bộ của cơ quan, tổ chức.

3. Hệ thống thông tin phục vụ người dân, doanh nghiệp là hệ thống trực tiếp hoặc hỗ trợ cung cấp dịch vụ trực tuyến, bao gồm dịch vụ công trực tuyến và dịch vụ trực tuyến khác trong các lĩnh vực viễn thông, công nghệ thông tin, thương mại, tài chính, ngân hàng, y tế, giáo dục và các lĩnh vực chuyên ngành khác.

4. Hệ thống cơ sở hạ tầng thông tin là tập hợp trang thiết bị, đường truyền dẫn kết nối phục vụ chung hoạt động của nhiều cơ quan, tổ chức như mạng diện

rộng, cơ sở dữ liệu, trung tâm dữ liệu, điện toán đám mây; xác thực điện tử, chứng thực điện tử, chữ ký số; kết nối liên thông các hệ thống thông tin.

5. Hệ thống thông tin Điều khiển công nghiệp là hệ thống có chức năng giám sát, thu thập dữ liệu, quản lý và kiểm soát các hạng mục quan trọng phục vụ điều khiển, vận hành hoạt động bình thường của các công trình xây dựng.

6. Hệ thống thông tin khác là hệ thống thông tin không thuộc các loại hình được nêu tại các khoản 2, 3, 4, 5 Điều này, được sử dụng để trực tiếp phục vụ hoặc hỗ trợ hoạt động nghiệp vụ, sản xuất, kinh doanh cụ thể của cơ quan, tổ chức theo lĩnh vực chuyên ngành.

7. Định kỳ hàng quý (ngày đầu tiên của quý), Cục An toàn thông tin – Bộ Thông tin và Truyền thông có trách nhiệm cập nhật, bổ sung danh mục các hệ thống thông tin theo quy định tại các khoản 2, 3, 4, 5, 6 Điều này và công bố trên Cổng thông tin điện tử của Bộ Thông tin và Truyền thông.

Điều 8. Thuyết minh cấp độ an toàn hệ thống thông tin

1. Đối với hệ thống thông tin được đầu tư xây dựng mới hoặc mở rộng, nâng cấp, tùy thuộc vào hình thức đầu tư, phương án kỹ thuật trong Báo cáo kinh tế - kỹ thuật (trường hợp dự án đầu tư áp dụng phương án thiết kế 01 bước), trong Thiết kế cơ sở thuộc Báo cáo nghiên cứu khả thi (trường hợp dự án đầu tư áp dụng phương án thiết kế 02 bước), trong Kế hoạch thuê dịch vụ công nghệ thông tin (trong trường hợp thuê dịch vụ công nghệ thông tin) hoặc trong Đề cương và dự toán chi tiết (trong trường hợp đầu tư ứng dụng công nghệ thông tin không phải lập dự án) phải đáp ứng các yêu cầu của phương án bảo đảm an toàn thông tin theo cấp độ được đề xuất, được thuyết minh trong Hồ sơ đề xuất cấp độ.

2. Thuyết minh Hồ sơ đề xuất cấp độ, bao gồm các thành phần sau đây:

a) Thuyết minh tổng quan về hệ thống thông tin;

b) Thuyết minh về việc đề xuất cấp độ;

c) Thuyết minh phương án bảo đảm an toàn thông tin.

3. Thuyết minh tổng quan về hệ thống thông tin, bao gồm các nội dung:

a) Thông tin về chủ quản hệ thống thông tin, gồm: tên chủ quản hệ thống thông tin; quy định chức năng, nhiệm vụ và quyền hạn; người đại diện, chức vụ; địa chỉ; thông tin liên hệ (bao gồm số điện thoại, thư điện tử);

b) Thông tin về đơn vị vận hành hệ thống thông tin, gồm: tên đơn vị vận hành; quy định chức năng, nhiệm vụ và quyền hạn; người đại diện, chức vụ; địa chỉ; thông tin liên hệ (bao gồm số điện thoại, thư điện tử);

c) Mô tả phạm vi, quy mô của hệ thống thông tin, trong đó cần làm rõ phạm vi của hệ thống, quy mô của hệ thống và đối tượng phục vụ của hệ thống;

d) Mô tả hiện trạng kiến trúc hệ thống (đối với hệ thống đang vận hành) hoặc mô tả kiến trúc hệ thống (đối với hệ thống được xây dựng mới hoặc nâng cấp, mở rộng), trong đó mô tả cụ thể mô hình lô-gic, mô hình vật lý của hệ thống, danh mục thiết bị và thiết bị mạng chính trong hệ thống (bao gồm tên thiết bị/chủng loại, vị trí triển khai, mục đích sử dụng), danh mục ứng dụng/dịch vụ cung cấp bởi hệ thống (bao gồm tên dịch vụ, máy chủ triển khai/vị trí triển khai/hệ điều hành máy chủ, mục đích sử dụng dịch vụ), quy hoạch các vùng mạng và địa chỉ IP trong hệ thống (bao gồm vùng mạng, đại chỉ IP nội bộ (IP Private), địa chỉ IP công khai (IP Public)).

4. Thuyết minh về việc đề xuất cấp độ, bao gồm các nội dung:

a) Danh mục các hệ thống thông tin và cấp độ tương ứng, bao gồm: tên hệ thống thông tin, cấp độ đề xuất, căn cứ đề xuất đối với từng hệ thống thông tin;

b) Thuyết minh chi tiết đối với các hệ thống thông tin, trong đó cần làm rõ loại thông tin được xử lý, loại hệ thống thông tin, căn cứ đề xuất cấp độ đối với từng hệ thống thông tin.

5. Thuyết minh về việc đề xuất cấp độ đối với hệ thống thông tin được đề xuất cấp độ 4 hoặc cấp độ 5, ngoài các nội dung được quy định tại khoản 3 Điều này, cần làm rõ thêm các nội dung sau đây:

a) Xác định các hệ thống thông tin khác có liên quan hoặc có kết nối đến hoặc có ảnh hưởng quan trọng tới hoạt động bình thường của hệ thống thông tin được đề xuất cấp độ;

b) Thuyết minh về các nguy cơ tấn công mạng và mức độ ảnh hưởng đối với hệ thống thông tin được đề xuất cấp độ;

c) Đánh giá phạm vi và mức độ ảnh hưởng tới lợi ích công cộng, trật tự an toàn xã hội hoặc quốc phòng, an ninh quốc gia khi bị tấn công mạng gây mất an toàn thông tin hoặc gián đoạn hoạt động của hệ thống thông tin được đề xuất cấp độ;

d) Thuyết minh yêu cầu cần phải vận hành 24/7 và không chấp nhận ngừng vận hành mà không có kế hoạch trước đối với các hệ thống thông tin theo quy định tại khoản 2 và khoản 3 Điều 10 của Nghị định 85/2016/NĐ-CP.

6. Thuyết minh phương án bảo đảm an toàn thông tin, bao gồm các nội dung:

a) Thuyết minh phương án đáp ứng các yêu cầu về quản lý tương ứng với cấp độ đề xuất;

b) Thuyết minh phương án đáp ứng các yêu cầu về kỹ thuật tương ứng với cấp độ đề xuất.

Chương III
YÊU CẦU BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN THEO CẤP ĐỘ

Điều 9. Yêu cầu chung

1. Việc bảo đảm an toàn hệ thống thông tin theo cấp độ thực hiện theo yêu cầu cơ bản quy định tại Thông tư này và Tiêu chuẩn quốc gia TCVN 11930:2017 về Công nghệ thông tin – các kỹ thuật an toàn – yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ.

2. Yêu cầu cơ bản đối với từng cấp độ quy định tại Thông tư này là các yêu cầu tối thiểu để bảo đảm an toàn hệ thống thông tin, bao gồm yêu cầu cơ bản về quản lý, yêu cầu cơ bản về kỹ thuật và không bao gồm các yêu cầu bảo đảm an toàn vật lý.

3. Yêu cầu cơ bản về quản lý, bao gồm:

a) Thiết lập chính sách an toàn thông tin;

b) Tổ chức bảo đảm an toàn thông tin;

c) Bảo đảm nguồn nhân lực;

d) Quản lý thiết kế, xây dựng hệ thống;

đ) Quản lý vận hành hệ thống;

e) Phương án Quản lý rủi ro an toàn thông tin;

g) Phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin.

4. Yêu cầu cơ bản về kỹ thuật, bao gồm:

a) Bảo đảm an toàn mạng;

b) Bảo đảm an toàn máy chủ;

c) Bảo đảm an toàn ứng dụng;

d) Bảo đảm an toàn dữ liệu.

5. Việc xây dựng phương án bảo đảm an toàn thông tin đáp ứng yêu cầu cơ bản theo từng cấp độ thực hiện theo nguyên tắc quy định tại khoản 2 Điều 4 Nghị định 85/2016/NĐ-CP, cụ thể như sau:

a) Đối với hệ thống thông tin cấp độ 1, 2, 3: Phương án bảo đảm an toàn thông tin phải xem xét khả năng dùng chung giữa các hệ thống thông tin đối với các giải pháp bảo vệ, chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư thừa, trùng lặp, lãng phí;

b) Đối với hệ thống thông tin cấp độ 4, 5: Phương án bảo đảm an toàn thông tin cần được thiết kế bảo đảm tính sẵn sàng, phân tách và hạn chế ảnh

hưởng đến toàn bộ hệ thống khi một thành phần trong hệ thống hoặc có liên quan tới hệ thống bị mất an toàn thông tin.

6. Hệ thống thông tin khi được đầu tư xây dựng mới hoặc mở rộng, nâng cấp phải triển khai đầy đủ phương án bảo đảm an toàn thông tin đã được phê duyệt tại Hồ sơ đề xuất cấp độ và đáp ứng các yêu cầu an toàn tại Điều 9 và Điều 10 Thông tư này trước khi đưa vào vận hành, khai thác.

7. Quy chế bảo đảm an toàn hệ thống thông tin cho hệ thống phải được xây dựng, đáp ứng các yêu cầu an toàn về quản lý theo cấp độ an toàn hệ thống thông tin tương ứng và được cấp có thẩm quyền phê duyệt, ban hành trước khi Hồ sơ đề xuất cấp độ được phê duyệt.

8. Yêu cầu bảo đảm an toàn thông tin đối với phần mềm nội bộ khi xây dựng mới hoặc mở rộng, nâng cấp:

a) Phần mềm nội bộ được xây dựng mới hoặc mở rộng, nâng cấp phải tuân thủ Khung phát triển phần mềm an toàn;

b) Đáp ứng yêu cầu an toàn cơ bản đối với Phần mềm nội bộ.

9. Trường hợp hệ thống thông tin cấp độ 3 được triển khai dưới hình thức thuê dịch vụ công nghệ thông tin tại Trung tâm dữ liệu hoặc Điện toán đám mây, thiết kế hệ thống phải đáp ứng các yêu cầu sau:

a) Phải được thiết kế tách riêng, độc lập với các hệ thống khác về lô-gic và có biện pháp quản lý truy cập giữa các hệ thống;

b) Các vùng mạng trong hệ thống phải được thiết kế tách riêng, độc lập với nhau về lô-gic và có biện pháp quản lý truy cập giữa các vùng mạng;

c) Có phân vùng lưu trữ được phân tách độc lập về lô-gic.

10. Trường hợp hệ thống thông tin cấp độ 4 hoặc cấp độ 5 được triển khai dưới hình thức thuê dịch vụ công nghệ thông tin tại Trung tâm dữ liệu hoặc Điện toán đám mây, thiết kế hệ thống phải đáp ứng các yêu cầu sau:

a) Phải được thiết kế tách riêng, độc lập với các hệ thống khác về vật lý và có biện pháp quản lý truy cập giữa các hệ thống;

b) Các vùng mạng trong hệ thống phải được thiết kế tách riêng, độc lập với nhau về lô-gic và có biện pháp quản lý truy cập giữa các vùng mạng;

c) Có phân vùng lưu trữ được phân tách độc lập về vật lý;

d) Các thiết bị mạng chính phải được phân tách độc lập về vật lý.

Điều 10. Phương án bảo đảm an toàn thông tin đối với từng cấp độ

1. Phương án bảo đảm an toàn hệ thống thông tin cấp độ 1 phải đáp ứng yêu cầu quy định chi tiết tại Phụ lục I ban hành kèm theo Thông tư này.

2. Phương án bảo đảm an toàn hệ thống thông tin cấp độ 2 phải đáp ứng yêu cầu quy định chi tiết tại Phụ lục II ban hành kèm theo Thông tư này.

3. Phương án bảo đảm an toàn hệ thống thông tin cấp độ 3 phải đáp ứng yêu cầu quy định chi tiết tại Phụ lục III ban hành kèm theo Thông tư này.

4. Phương án bảo đảm an toàn hệ thống thông tin cấp độ 4 phải đáp ứng yêu cầu quy định chi tiết tại Phụ lục IV ban hành kèm theo Thông tư này.

5. Phương án bảo đảm an toàn hệ thống thông tin cấp độ 5 phải đáp ứng yêu cầu quy định chi tiết tại Phụ lục V ban hành kèm theo Thông tư này.

Chương IV
KIỂM TRA, ĐÁNH GIÁ AN TOÀN THÔNG TIN

Điều 11. Quy định chung về hoạt động kiểm tra, đánh giá

1. Nội dung kiểm tra, đánh giá:

a) Kiểm tra, đánh giá việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ;

b) Kiểm tra, đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin theo phương án bảo đảm an toàn thông tin được phê duyệt;

c) Kiểm tra, đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thông tin.

2. Tần suất kiểm tra, đánh giá:

a) Kiểm tra, đánh giá định kỳ theo quy định tại điểm c khoản 2 Điều 20 Nghị định 85/2016/NĐ-CP;

b) Kiểm tra, đánh giá đột xuất theo yêu cầu của cấp có thẩm quyền.

3. Hình thức kiểm tra, đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thông tin, gồm 03 hình thức sau:

a) Kiểm tra, đánh giá hộp đen (Black box);

b) Kiểm tra, đánh giá hộp xám (Gray box);

c) Kiểm tra, đánh giá hộp trắng (White box).

Điều 12. Nội dung kiểm tra, đánh giá về an toàn thông tin

1. Nội dung kiểm tra, đánh giá việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ, bao gồm:

a) Kiểm tra, đánh giá tuân thủ đối với Chủ quản hệ thống thông tin theo quy định tại Điều 20 Nghị định 85/2016/NĐ-CP, bao gồm: việc thực hiện thành lập/chỉ định đơn vị chuyên trách/bộ phận chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin theo quy định tại khoản 1 Điều 20 Nghị định 85/2016/NĐ-CP; việc thực hiện lập Hồ sơ đề xuất cấp độ, tổ chức thẩm định, phê duyệt Hồ sơ đề xuất cấp độ theo quy định đối với các hệ thống thông tin thuộc phạm vi quản lý; việc triển khai phương án bảo đảm an toàn thông tin theo

phương án trong Hồ sơ đề xuất cấp độ được phê duyệt đối với các hệ thống thông tin thuộc phạm vi quản lý; việc tổ chức thực hiện kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin trong phạm vi cơ quan, tổ chức mình theo quy định tại điểm c khoản 2 Điều 20 Nghị định 85/2016/NĐ-CP; việc tổ chức thực hiện đào tạo ngắn hạn, tuyên truyền, phổ biến, nâng cao nhận thức và diễn tập về an toàn thông tin theo quy định tại điểm d Khoản 2 Điều 20 Nghị định 85/2016/NĐ-CP;

b) Kiểm tra, đánh giá tuân thủ đối với Đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin theo quy định tại Điều 21 Nghị định 85/2016/NĐ-CP, bao gồm các nội dung: công tác tham mưu, tổ chức thực thi, đôn đốc, kiểm tra, giám sát công tác bảo đảm an toàn thông tin; công tác thẩm định, phê duyệt hoặc cho ý kiến về mặt chuyên môn đối với Hồ sơ đề xuất cấp độ theo thẩm quyền quy định;

c) Kiểm tra, đánh giá tuân thủ đối với Đơn vị vận hành theo quy định tại Điều 22 Nghị định 85/2016/NĐ-CP;

d) Kiểm tra, đánh giá việc tổ chức thực thi các biện pháp bảo đảm an toàn thông tin theo phương án bảo đảm an toàn thông tin được phê duyệt.

2. Nội dung kiểm tra, đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin theo phương án bảo đảm an toàn thông tin được phê duyệt, bao gồm:

a) Kiểm tra tính đầy đủ và phù hợp của Quy chế bảo đảm an toàn thông tin theo phương án bảo đảm an toàn thông tin về quản lý được phê duyệt;

b) Đánh giá việc tuân thủ các quy định, quy trình trong Quy chế bảo đảm an toàn thông tin trong quá trình vận hành, khai thác, kết thúc hoặc hủy bỏ hệ thống thông tin;

c) Đánh giá việc thiết kế hệ thống theo phương án bảo đảm an toàn thông tin được phê duyệt;

d) Đánh giá việc thiết lập, cấu hình hệ thống theo phương án bảo đảm an toàn thông tin được phê duyệt;

đ) Kiểm tra việc cấu hình, tăng cường bảo mật cho thiết bị hệ thống, hệ điều hành, ứng dụng, cơ sở dữ liệu và các thành phần khác liên quan trong hệ thống theo hướng dẫn của Bộ Thông tin và Truyền thông.

3. Nội dung kiểm tra, đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thông tin, bao gồm:

a) Dò quét, phát hiện mã độc, lỗ hổng, điểm yếu của hệ thống, thử nghiệm tấn công xâm nhập đối với các thiết bị hệ thống, hệ điều hành, ứng dụng, cơ sở dữ liệu và các thành phần khác liên quan trong hệ thống;

b) Đánh giá an toàn mã nguồn đối với phần mềm nội bộ;

c) Đưa ra phương án và kế hoạch xử lý lỗ hổng, điểm yếu và phương án cấu hình, tăng cường bảo mật đối với các nội dung kiểm tra được đánh giá là chưa đạt.

Chương V
CHẾ ĐỘ BÁO CÁO

Điều 13. Quy định chung về chế độ báo cáo

1. Phương thức gửi, nhận báo cáo:

a) Gửi qua hệ thống quản lý văn bản và điều hành;

b) Gửi qua hệ thống phần mềm báo cáo do Bộ Thông tin và Truyền thông triển khai;

c) Gửi qua hệ thống thư điện tử;

d) Các phương thức khác theo quy định của pháp luật.

2. Tần suất thực hiện báo cáo:

a) Định kỳ hàng năm;

b) Đột xuất theo đề nghị của cơ quan có thẩm quyền.

3. Thời gian chốt số liệu báo cáo định kỳ hàng năm:

Tính từ ngày 15 tháng 12 năm trước kỳ báo cáo đến ngày 14 tháng 12 của kỳ báo cáo.

4. Thời hạn gửi báo cáo đối với báo cáo định kỳ hàng năm:

a) Đơn vị chuyên trách về an toàn thông tin, đơn vị vận hành hệ thống thông tin gửi báo cáo tới chủ quản hệ thống thông tin trước ngày 20 tháng 12 hàng năm;

b) Chủ quản hệ thống thông tin gửi báo cáo Bộ Thông tin và Truyền thông trước ngày 25 tháng 12 hàng năm.

Điều 14. Nội dung báo cáo

1. Thông tin chung về chủ quản hệ thống thông tin, đơn vị chuyên trách về an toàn thông tin, đơn vị vận hành đối với từng hệ thống thông thông tin thuộc phạm vi quản lý, gồm: tên chủ quản hệ thống thông tin, đơn vị chuyên trách an toàn thông tin, đơn vị vận hành; quy định chức năng, nhiệm vụ và quyền hạn; người đại diện, chức vụ; địa chỉ; thông tin liên hệ (bao gồm số điện thoại, thư điện tử).

2. Danh sách các hệ thống thông tin thuộc phạm vi quản lý, gồm: tên hệ thống, đơn vị vận hành, cấp độ đề xuất.

3. Danh sách hệ thống thông tin được phê duyệt Hồ sơ đề xuất cấp độ theo quy định.

4. Danh sách hệ thống thông tin đã triển khai đầy đủ, mới triển khai một phần hoặc chưa triển khai các biện pháp bảo vệ đáp ứng các yêu cầu an toàn theo phương án bảo đảm an toàn thông tin theo cấp độ đã được phê duyệt.

5. Danh sách hệ thống thông tin có Quy chế bảo đảm an toàn thông tin theo quy định.

6. Danh sách hệ thống thông tin tuân thủ các quy định, quy trình trong Quy chế bảo đảm an toàn thông tin trong quá trình vận hành, khai thác, kết thúc hoặc hủy bỏ hệ thống thông tin.

7. Danh sách hệ thống thông tin được kiểm tra, đánh giá theo quy định.

8. Đánh giá về việc triển khai các biện pháp bảo đảm an toàn thông tin theo phương án bảo đảm an toàn thông tin được phê duyệt trong Hồ sơ đề xuất cấp độ theo từng tiêu chí, yêu cầu.

9. Thông tin Quyết định phê duyệt Hồ sơ đề xuất cấp độ, phương án bảo đảm an toàn thông tin được phê duyệt trong Hồ sơ đề xuất cấp độ theo từng tiêu chí, yêu cầu (đã đáp ứng đầy đủ/chưa đáp ứng đầy đủ; kế hoạch hoặc lộ trình hoàn thiện tiêu chí, yêu cầu chưa đáp ứng).

10. Thông tin Quyết định ban hành và Quy chế bảo đảm an toàn thông tin.

11. Các thông tin khác theo yêu cầu của cơ quan có thẩm quyền.

Chương VI
TỔ CHỨC THỰC HIỆN

Điều 15. Thời điểm phê duyệt Hồ sơ đề xuất cấp độ khi xây dựng mới hoặc mở rộng, nâng cấp hệ thống thông tin

Hồ sơ đề xuất cấp độ an toàn thông tin khuyến khích được phê duyệt trước khi cấp có thẩm quyền phê duyệt Báo cáo kinh tế - kỹ thuật hoặc thiết kế cơ sở thuộc Báo cáo nghiên cứu khả thi hoặc Kế hoạch thuê dịch vụ công nghệ thông tin hoặc Đề cương và dự toán chi tiết tương ứng.

Điều 16. Điều khoản chuyển tiếp

1. Đối với các hệ thống thông tin đang vận hành, khai thác, đã được phê duyệt cấp độ từ trước ngày Thông tư này có hiệu lực: Chủ quản hệ thống thông tin tiến hành rà soát Hồ sơ đề xuất cấp độ và Phương án đảm bảo an toàn thông tin đã được phê duyệt. Việc rà soát, điều chỉnh, phê duyệt lại Hồ sơ đề xuất cấp độ và Phương án bảo đảm an toàn thông tin (nếu cần) phải hoàn thành trước tháng 6 năm 2023.

2. Đối với các hệ thống thông tin đang vận hành, khai thác nhưng chưa được phê duyệt Hồ sơ đề xuất cấp độ: thực hiện xây dựng, thẩm định, phê duyệt Hồ sơ đề xuất cấp độ và triển khai phương án bảo đảm an toàn thông tin theo

phương án được phê duyệt trong Hồ sơ đề xuất cấp độ đáp ứng các yêu cầu theo quy định tại Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 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 bảo đảm an toàn hệ thống thông tin theo cấp độ và đồng bộ với quy định tại Thông tư này, bảo đảm khi Thông tư này có hiệu lực, không phải thực hiện lại quy trình xây dựng, thẩm định, phê duyệt Hồ sơ đề xuất cấp độ.

Điều 17. Hiệu lực và trách nhiệm thi hành

1. Thông tư này có hiệu lực từ ngày 01 tháng 10 năm 2022 và thay thế cho Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 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 bảo đảm an toàn hệ thống thông tin theo cấp độ.

2. Trong quá trình thực hiện Thông tư này, nếu có vướng mắc, các cơ quan, đơn vị liên hệ với Bộ Thông tin và Truyền thông (Cục An toàn thông tin) để phối hợp giải quyết./.

Nơi nhận:
- Thủ tướng và các Phó Thủ tướng Chính phủ (để b/c);
- Văn phòng Trung ương và các Ban của Đảng;
- Văn phòng Tổng Bí thư;
- Văn phòng Quốc hội;
- Văn phòng Chủ tịch nước;
- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Tòa án nhân dân tối cao;
- Viện Kiểm sát nhân dân tối cao;
- Kiểm toán Nhà nước;
- Các cơ quan Trung ương của các đoàn thể;
- UBND các tỉnh, thành phố trực thuộc Trung ương;
- Cục Kiểm tra văn bản QPPL (Bộ Tư pháp);
- Sở TTTT các tỉnh, thành phố trực thuộc Trung ương;
- Công báo, Cổng thông tin điện tử Chính phủ;
- Bộ TTTT: Bộ trưởng và các Thứ trưởng; các cơ quan, đơn vị thuộc Bộ; Cổng Thông tin điện tử;
- Lưu: VT, CATTT (230).

BỘ TRƯỞNG

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Mạnh Hùng

Phụ lục I

YÊU CẦU CƠ BẢN BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN ĐỐI VỚI HỆ THỐNG THÔNG TIN CẤP ĐỘ 1

(Ban hành kèm theo Thông tư số 12 /2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ trưởng Bộ Thông tin và Truyền thông)

I. YÊU CẦU QUẢN LÝ

STT	Yêu cầu	TCVN 11930:2017
1.1	**Thiết lập chính sách an toàn thông tin**	**Mục 5.1.1**
1.1.1	Chính sách an toàn thông tin	Mục 5.1.1.1
1.1.2	Xây dựng và công bố	Mục 5.1.1.2
1.1.3	Rà soát, sửa đổi	Mục 5.1.1.3
1.2	**Tổ chức bảo đảm an toàn thông tin**	**Mục 5.1.2**
1.2.1	Đơn vị chuyên trách về an toàn thông tin	Mục 5.1.2.1
1.2.2	Phối hợp với cơ quan/tổ chức có thẩm quyền	Mục 5.1.2.2
1.3	**Bảo đảm nguồn nhân lực**	**Mục 5.1.3**
1.3.1	Tuyển dụng	Mục 5.1.3.1
1.3.2	Trong quá trình làm việc	Mục 5.1.3.2
1.3.3	Chấm dứt hoặc thay đổi công việc	Mục 5.1.3.3
1.4	**Quản lý thiết kế, xây dựng hệ thống**	**Mục 5.1.4**
1.4.1	Thiết kế an toàn hệ thống thông tin	Mục 5.1.4.1
1.4.2	Thử nghiệm và nghiệm thu hệ thống	Mục 5.1.4.2
1.5	**Quản lý vận hành hệ thống**	**Mục 5.1.5**
1.5.1	Quản lý an toàn mạng	Mục 5.1.5.1
1.5.2	Quản lý an toàn máy chủ và ứng dụng	Mục 5.1.5.2
1.5.3	Quản lý an toàn dữ liệu	Mục 5.1.5.3
1.6	**Phương án Quản lý rủi ro an toàn thông tin**	
1.7	**Phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ**	

II. YÊU CẦU KỸ THUẬT

1. Yêu cầu về thiết kế hệ thống

a) Thiết kế các vùng mạng trong hệ thống theo chức năng, các vùng mạng tối thiểu bao gồm:

i. Vùng mạng nội bộ;

ii. Vùng mạng biên;

iii. Vùng DMZ.

b) Có phương án thiết kế bảo đảm các yêu cầu sau:

i. Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn sử dụng mạng riêng ảo hoặc phương án tương đương;

ii. Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập, sử dụng sản phẩm Tường lửa có tích hợp chức năng phòng, chống xâm nhập hoặc phương án tương đương;

iii. Có phương án phòng chống mã độc cho máy chủ và máy trạm sử dụng sản phẩm Phòng chống mã độc hoặc phương án tương đương.

2. Yêu cầu về thiết lập, cấu hình hệ thống

STT	Yêu cầu	TCVN 11930:2017
1.1	**Bảo đảm an toàn mạng**	**Mục 5.2.1**
1.1.1	Kiểm soát truy cập từ bên ngoài mạng	Mục 5.2.1.2
1.1.2	Nhật kí hệ thống	Mục 5.2.1.3
1.1.3	Phòng chống xâm nhập	Mục 5.2.1.4
1.1.4	Bảo vệ thiết bị hệ thống	Mục 5.2.1.5
1.2	**Bảo đảm an toàn máy chủ**	**Mục 5.2.2**
1.2.1	Xác thực	Mục 5.2.2.1
1.2.2	Kiểm soát truy cập	Mục 5.2.2.2
1.2.3	Nhật ký hệ thống	Mục 5.2.2.3
1.2.4	Phòng chống xâm nhập	Mục 5.2.2.4
1.2.5	Phòng chống phần mềm độc hại	Mục 5.2.2.5
1.3	**Bảo đảm an toàn ứng dụng**	**Mục 5.2.3**
1.3.1	Xác thực	Mục 5.2.3.1
1.3.2	Kiểm soát truy cập	Mục 5.2.3.2
1.3.3	Nhật kí hệ thống	Mục 5.2.3.3
1.4	**Bảo đảm an toàn dữ liệu**	**Mục 5.2.4**
1.4.1	Sao lưu dự phòng	Mục 5.2.4.1

Phụ lục II

YÊU CẦU CƠ BẢN BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN ĐỐI VỚI HỆ THỐNG THÔNG TIN CẤP ĐỘ 2

(Ban hành kèm theo Thông tư số 12 /2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ trưởng Bộ Thông tin và Truyền thông)

I. YÊU CẦU QUẢN LÝ

STT	Yêu cầu	TCVN 11930:2017
1.1	**Thiết lập chính sách an toàn thông tin**	**Mục 6.1.1**
1.1.1	Chính sách an toàn thông tin	Mục 6.1.1.1
1.1.2	Xây dựng và công bố	Mục 6.1.1.2
1.1.3	Rà soát, sửa đổi	Mục 6.1.1.3
1.2	**Tổ chức bảo đảm an toàn thông tin**	**Mục 6.1.2**
1.2.1	Đơn vị chuyên trách về an toàn thông tin	Mục 6.1.2.1
1.2.2	Phối hợp với cơ quan/tổ chức có thẩm quyền	Mục 6.1.2.2
1.3	**Bảo đảm nguồn nhân lực**	**Mục 6.1.3**
1.3.1	Tuyển dụng	Mục 6.1.3.1
1.3.2	Trong quá trình làm việc	Mục 6.1.3.2
1.3.3	Chấm dứt hoặc thay đổi công việc	Mục 6.1.3.3
1.4	**Quản lý thiết kế, xây dựng hệ thống**	**Mục 6.1.4**
1.4.1	Thiết kế an toàn hệ thống thông tin	Mục 6.1.4.1
1.4.2	Phát triển phần mềm thuê khoán	Mục 6.1.4.2
1.4.3	Thử nghiệm và nghiệm thu hệ thống	Mục 6.1.4.3
1.5	**Quản lý vận hành hệ thống**	**Mục 6.1.5**
1.5.1	Quản lý an toàn mạng	Mục 6.1.5.1
1.5.2	Quản lý an toàn máy chủ và ứng dụng	Mục 6.1.5.2
1.5.3	Quản lý an toàn dữ liệu	Mục 6.1.5.3
1.5.4	Quản lý sự cố an toàn thông tin	Mục 6.1.5.4
1.5.5	Quản lý an toàn người sử dụng đầu cuối	Mục 6.1.5.5
1.6	**Phương án Quản lý rủi ro an toàn thông tin**	
1.7	**Phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ**	

II. YÊU CẦU KỸ THUẬT

1. Yêu cầu về thiết kế hệ thống

a) Thiết kế các vùng mạng trong hệ thống theo chức năng, các vùng mạng tối thiểu bao gồm:

i. Vùng mạng nội bộ;

ii. Vùng mạng biên;

iii. Vùng DMZ;

iv. Vùng máy chủ nội bộ;

v. Vùng mạng không dây (nếu có) tách riêng, độc lập với các vùng mạng khác.

b) Có phương án thiết kế bảo đảm các yêu cầu sau:

i. Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn sử dụng mạng riêng ảo hoặc phương án tương đương;

ii. Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập, sử dụng sản phẩm Tường lửa có tích hợp chức năng phòng, chống xâm nhập hoặc phương án tương đương;

iii. Có phương án phòng chống mã độc cho máy chủ và máy trạm sử dụng sản phẩm Phòng chống mã độc hoặc phương án tương đương;

iv. Có phương án phòng chống tấn công mạng cho ứng dụng web; sử dụng sản phẩm Tường lửa ứng dụng web đối với hệ thống thông tin theo quy định tại khoản 2 Điều 8 Nghị định 85/2016/NĐ-CP;

v. Có phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử đối với hệ thống thư điện tử;

vi. Có phương án dự phòng cho các thiết bị mạng chính, bao gồm thiết bị chuyển mạch trung tâm hoặc tương đương, thiết bị tường lửa trung tâm.

2. Yêu cầu về thiết lập, cấu hình hệ thống

STT	Yêu cầu	TCVN 11930:2017
1.1	**Bảo đảm an toàn mạng**	**Mục 6.2.1**
1.1.1	Kiểm soát truy cập từ bên ngoài mạng	Mục 6.2.1.2
1.1.2	Kiểm soát truy cập từ bên trong mạng	Mục 6.2.1.3
1.1.3	Nhật kí hệ thống	Mục 6.2.1.4
1.1.4	Phòng chống xâm nhập	Mục 6.2.1.5
1.1.5	Bảo vệ thiết bị hệ thống	Mục 6.2.1.6
1.2	**Bảo đảm an toàn máy chủ**	**Mục 6.2.2**

1.2.1	Xác thực	Mục 6.2.2.1
1.2.2	Kiểm soát truy cập	Mục 6.2.2.2
1.2.3	Nhật ký hệ thống	Mục 6.2.2.3
1.2.4	Phòng chống xâm nhập	Mục 6.2.2.4
1.2.5	Phòng chống phần mềm độc hại	Mục 6.2.2.5
1.2.6	Xử lý máy chủ khi chuyển giao	Mục 6.2.2.6
1.3	**Bảo đảm an toàn ứng dụng**	**Mục 6.2.3**
1.3.1	Xác thực	Mục 6.2.3.1
1.3.2	Kiểm soát truy cập	Mục 6.2.3.2
1.3.3	Nhật kí hệ thống	Mục 6.2.3.3
1.3.4	An toàn ứng dụng và mã nguồn	Mục 6.2.3.4
1.4	**Bảo đảm an toàn dữ liệu**	**Mục 6.2.4**
1.4.1	Bảo mật dữ liệu	Mục 6.2.4.1
1.4.2	Sao lưu dự phòng	Mục 6.2.4.2

Phụ lục III
YÊU CẦU CƠ BẢN BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN ĐỐI VỚI HỆ THỐNG THÔNG TIN CẤP ĐỘ 3

(Ban hành kèm theo Thông tư số /2022/TT-BTTTT ngày tháng năm 2022 của Bộ trưởng Bộ Thông tin và Truyền thông)

I. YÊU CẦU QUẢN LÝ

STT	Yêu cầu	TCVN 11930:2017
1.1	**Thiết lập chính sách an toàn thông tin**	**Mục 7.1.1**
1.1.1	Chính sách an toàn thông tin	Mục 7.1.1.1
1.1.2	Xây dựng và công bố	Mục 7.1.1.2
1.1.3	Rà soát, sửa đổi	Mục 7.1.1.3
1.2	**Tổ chức bảo đảm an toàn thông tin**	**Mục 7.1.2**
1.2.1	Đơn vị chuyên trách về an toàn thông tin	Mục 7.1.2.1
1.2.2	Phối hợp với cơ quan/tổ chức có thẩm quyền	Mục 7.1.2.2
1.3	**Bảo đảm nguồn nhân lực**	**Mục 7.1.3**
1.3.1	Tuyển dụng	Mục 7.1.3.1
1.3.2	Trong quá trình làm việc	Mục 7.1.3.2
1.3.3	Chấm dứt hoặc thay đổi công việc	Mục 7.1.3.3
1.4	**Quản lý thiết kế, xây dựng hệ thống**	**Mục 7.1.4**
1.4.1	Thiết kế an toàn hệ thống thông tin	Mục 7.1.4.1
1.4.2	Phát triển phần mềm thuê khoán	Mục 7.1.4.2
1.4.3	Thử nghiệm và nghiệm thu hệ thống	Mục 7.1.4.3
1.5	**Quản lý vận hành hệ thống**	**Mục 7.1.5**
1.5.1	Quản lý an toàn mạng	Mục 7.1.5.1
1.5.2	Quản lý an toàn máy chủ và ứng dụng	Mục 7.1.5.2
1.5.3	Quản lý an toàn dữ liệu	Mục 7.1.5.3
1.5.4	Quản lý an toàn thiết bị đầu cuối	Mục 7.1.5.4
1.5.5	Quản lý phòng chống phần mềm độc hại	Mục 7.1.5.5
1.5.6	Quản lý giám sát an toàn hệ thống thông tin	Mục 7.1.5.6
1.5.7	Quản lý điểm yếu an toàn thông tin	Mục 7.1.5.7
1.5.8	Quản lý sự cố an toàn thông tin	Mục 7.1.5.8
1.5.9	Quản lý an toàn người sử dụng đầu cuối	Mục 7.1.5.9

1.6	**Phương án Quản lý rủi ro an toàn thông tin**
1.7	**Phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ**

II. YÊU CẦU KỸ THUẬT

1. Yêu cầu về thiết kế hệ thống

a) Thiết kế các vùng mạng trong hệ thống theo chức năng, các vùng mạng tối thiểu bao gồm:

i. Vùng mạng nội bộ;

ii. Vùng mạng biên;

iii. Vùng DMZ;

iv. Vùng máy chủ nội bộ;

v. Vùng mạng không dây (nếu có) tách riêng, độc lập với các vùng mạng khác;

vi. Vùng mạng máy chủ cơ sở dữ liệu;

vii. Vùng quản trị.

b) Có phương án thiết kế bảo đảm các yêu cầu sau:

i. Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn sử dụng mạng riêng ảo hoặc phương án tương đương; sử dụng sản phẩm Mạng riêng ảo đối với hệ thống thông tin có xử lý thông tin bí mật nhà nước hoặc hệ thống thông tin quy định tại điểm c khoản 2 Điều 9 Nghị định 85/2016/NĐ-CP;

ii. Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập sử dụng sản phẩm Tường lửa có tích hợp chức năng phòng, chống xâm nhập hoặc sản phẩm Phòng, chống xâm nhập lớp mạng;

iii. Có phương án cân bằng tải, dự phòng nóng cho các thiết bị mạng chính, tối thiểu bao gồm thiết bị chuyển mạch trung tâm hoặc tương đương, thiết bị tường lửa trung tâm, tường lửa ứng dụng web, hệ thống lưu trữ tập trung, tường lửa cơ sở dữ liệu (nếu có);

iv. Có phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu; sử dụng sản phẩm Tường lửa cơ sở dữ liệu đối với hệ thống cơ sở dữ liệu tập trung, đáp ứng tiêu chí quy định tại khoản 3 Điều 9 Nghị định 85/2016/NĐ-CP;

v. Có phương án chặn lọc phần mềm độc hại trên môi trường mạng sử dụng Tường lửa tích hợp chức năng phòng, chống mã độc trên môi trường mạng hoặc phương án tương đương;

vi. Có phương án phòng chống tấn công từ chối dịch vụ; sử dụng dịch vụ của doanh nghiệp hoặc sản phẩm Phòng, chống tấn công từ chối dịch vụ đối với các hệ thống Trung tâm dữ liệu, điện toán đám mây, hệ thống Định danh, xác thực điện tử, chứng thực điện tử, chữ ký số và hệ thống Kết nối tích hợp, chia sẻ

dữ liệu, đáp ứng tiêu chí quy định tại khoản 3 Điều 9 Nghị định 85/2016/NĐ-CP;

vii. Có phương án phòng chống tấn công mạng cho ứng dụng web; sử dụng sản phẩm Tường lửa ứng dụng web đối với các hệ thống thông tin được quy định tại khoản 2, Điều 9 Nghị định 85/2016/NĐ-CP;

viii. Có phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử; sử dụng sản phẩm Bảo đảm an toàn thông tin cho hệ thống thư điện tử đối với hệ thống Thư điện tử, đáp ứng tiêu chí quy định tại khoản 2 Điều 9 Nghị định 85/2016/NĐ-CP;

ix. Có phương án quản lý truy cập lớp mạng; sử dụng sản phẩm Quản lý truy cập lớp mạng đối với hệ thống Mạng nội bộ, Trung tâm giám sát điều hành an toàn thông tin mạng, đáp ứng tiêu chí quy định tại khoản 3 Điều 9 Nghị định 85/2016/NĐ-CP;

x. Có phương án giám sát hệ thống thông tin tập trung;

xi. Có phương án giám sát an toàn hệ thống thông tin tập trung sử dụng sản phẩm Quản lý và phân tích sự kiện an toàn thông tin hoặc sản phẩm tương đương;

xii. Có phương án quản lý sao lưu dự phòng tập trung sử dụng hệ thống lưu trữ tập trung và sản phẩm quản lý lưu trữ tập trung;

xiii. Có phương án quản lý phần mềm phòng chống mã độc trên máy chủ/máy tính người dùng, sử dụng sản phẩm Phòng, chống mã độc và/hoặc sản phẩm Phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu cuối, có chức năng quản lý tập trung;

xiv. Có phương án phòng, chống thất thoát dữ liệu; sử dụng sản phẩm Phòng, chống thất thoát dữ liệu đối với hệ thống thông tin có xử lý thông tin bí mật nhà nước hoặc hệ thống thông tin quy định tại điểm c khoản 2 Điều 9 Nghị định 85/2016/NĐ-CP;

xv. Có phương án dự phòng kết nối mạng Internet cho các máy chủ dịch vụ;

xvi. Có phương án bảo đảm an toàn cho mạng không dây (nếu có).

2. Yêu cầu về thiết lập, cấu hình hệ thống

STT	Yêu cầu	TCVN 11930:2017
1.1	**Bảo đảm an toàn mạng**	**Mục 7.2.1**
1.1.1	Kiểm soát truy cập từ bên ngoài mạng	Mục 7.2.1.2
1.1.2	Kiểm soát truy cập từ bên trong mạng	Mục 7.2.1.3
1.1.3	Nhật kí hệ thống	Mục 7.2.1.4

1.1.4	Phòng chống xâm nhập	Mục 7.2.1.5
1.1.5	Phòng chống phần mềm độc hại trên môi trường mạng	Mục 7.2.1.6
1.1.6	Bảo vệ thiết bị hệ thống	Mục 7.2.1.7
1.2	**Bảo đảm an toàn máy chủ**	**Mục 7.2.2**
1.2.1	Xác thực	Mục 7.2.2.1
1.2.2	Kiểm soát truy cập	Mục 7.2.2.2
1.2.3	Nhật ký hệ thống	Mục 7.2.2.3
1.2.4	Phòng chống xâm nhập	Mục 7.2.2.4
1.2.5	Phòng chống phần mềm độc hại	Mục 7.2.2.5
1.2.6	Xử lý máy chủ khi chuyển giao	Mục 7.2.2.6
1.3	**Bảo đảm an toàn ứng dụng**	**Mục 7.2.3**
1.3.1	Xác thực	Mục 7.2.3.1
1.3.2	Kiểm soát truy cập	Mục 7.2.3.2
1.3.3	Nhật kí hệ thống	Mục 7.2.3.3
1.3.4	Bảo mật thông tin liên lạc	Mục 7.2.3.4
1.3.5	Chống chối bỏ	Mục 7.2.3.5
1.3.6	An toàn ứng dụng và mã nguồn	Mục 7.2.3.6
1.4	**Bảo đảm an toàn dữ liệu**	**Mục 7.2.4**
1.4.1	Nguyên vẹn dữ liệu	Mục 7.2.4.1
1.4.2	Bảo mật dữ liệu	Mục 7.2.4.2
1.4.3	Sao lưu dự phòng	Mục 7.2.4.3

Phụ lục IV

YÊU CẦU CƠ BẢN BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN ĐỐI VỚI HỆ THỐNG THÔNG TIN CẤP ĐỘ 4

(Ban hành kèm theo Thông tư số /2022/TT-BTTTT ngày tháng năm 2022 của Bộ trưởng Bộ Thông tin và Truyền thông)

I. YÊU CẦU QUẢN LÝ

STT	Yêu cầu	TCVN 11930:2017
1.1	**Thiết lập chính sách an toàn thông tin**	**Mục 8.1.1**
1.1.1	Chính sách an toàn thông tin	Mục 8.1.1.1
1.1.2	Xây dựng và công bố	Mục 8.1.1.2
1.1.3	Rà soát, sửa đổi	Mục 8.1.1.3
1.2	**Tổ chức bảo đảm an toàn thông tin**	**Mục 8.1.2**
1.2.1	Đơn vị chuyên trách về an toàn thông tin	Mục 8.1.2.1
1.2.2	Phối hợp với cơ quan/tổ chức có thẩm quyền	Mục 8.1.2.2
1.3	**Bảo đảm nguồn nhân lực**	**Mục 8.1.3**
1.3.1	Tuyển dụng	Mục 8.1.3.1
1.3.2	Trong quá trình làm việc	Mục 8.1.3.2
1.3.3	Chấm dứt hoặc thay đổi công việc	Mục 8.1.3.3
1.4	**Quản lý thiết kế, xây dựng hệ thống**	**Mục 8.1.4**
1.4.1	Thiết kế an toàn hệ thống thông tin	Mục 8.1.4.1
1.4.2	Phát triển phần mềm thuê khoán	Mục 8.1.4.2
1.4.3	Thử nghiệm và nghiệm thu hệ thống	Mục 8.1.4.3
1.5	**Quản lý vận hành hệ thống**	**Mục 8.1.5**
1.5.1	Quản lý an toàn mạng	Mục 8.1.5.1
1.5.2	Quản lý an toàn máy chủ và ứng dụng	Mục 8.1.5.2
1.5.3	Quản lý an toàn dữ liệu	Mục 8.1.5.3
1.5.4	Quản lý an toàn thiết bị đầu cuối	Mục 8.1.5.4
1.5.5	Quản lý phòng chống phần mềm độc hại	Mục 8.1.5.5
1.5.6	Quản lý giám sát an toàn hệ thống thông tin	Mục 8.1.5.6
1.5.7	Quản lý điểm yếu an toàn thông tin	Mục 8.1.5.7
1.5.8	Quản lý sự cố an toàn thông tin	Mục 8.1.5.8
1.5.9	Quản lý an toàn người sử dụng đầu cuối	Mục 8.1.5.9

1.6	**Phương án Quản lý rủi ro an toàn thông tin**
1.7	**Phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ**

II. YÊU CẦU KỸ THUẬT

1. Yêu cầu về thiết kế hệ thống

a) Thiết kế các vùng mạng trong hệ thống theo chức năng, các vùng mạng tối thiểu bao gồm:

i. Vùng mạng nội bộ;

ii. Vùng mạng biên;

iii. Vùng DMZ;

iv. Vùng máy chủ nội bộ;

v. Vùng mạng không dây (nếu có) tách riêng, độc lập với các vùng mạng khác;

vi. Vùng mạng máy chủ cơ sở dữ liệu;

vii. Vùng quản trị;

viii. Vùng quản trị thiết bị hệ thống.

b) Có phương án thiết kế bảo đảm các yêu cầu sau:

i. Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn sử dụng mạng riêng ảo hoặc phương án tương đương; sử dụng sản phẩm Mạng riêng ảo đối với hệ thống thông tin có xử lý thông tin bí mật nhà nước;

ii. Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập sử dụng sản phẩm Tường lửa có tích hợp chức năng phòng, chống xâm nhập hoặc sản phẩm Phòng, chống xâm nhập lớp mạng;

iii. Có phương án cân bằng tải, dự phòng nóng cho các thiết bị mạng chính, tối thiểu bao gồm thiết bị chuyển mạch trung tâm hoặc tương đương, thiết bị tường lửa trung tâm, tường lửa ứng dụng web, hệ thống lưu trữ tập trung, tường lửa cơ sở dữ liệu (nếu có);

iv. Có phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu; sử dụng sản phẩm Tường lửa cơ sở dữ liệu đối với hệ thống Cơ sở dữ liệu dùng chung đáp ứng tiêu chí quy định tại khoản 3 Điều 10 Nghị định 85/2016/NĐ-CP;

v. Có phương án chặn lọc phần mềm độc hại trên môi trường mạng sử dụng Sản phẩm Tường lửa tích hợp chức năng phòng, chống mã độc trên môi trường mạng hoặc phương án tương đương;

vi. Có phương án phòng chống tấn công từ chối dịch vụ; sử dụng dịch vụ của doanh nghiệp hoặc sản phẩm Phòng, chống tấn công từ chối dịch vụ đối với các hệ thống thông tin được quy định tại khoản 2 Điều 10 Nghị định

85/2016/NĐ-CP hoặc Hệ thống Trung tâm dữ liệu, điện toán đám mây, Định danh, xác thực điện tử, chứng thực điện tử, chữ ký số, Kết nối tích hợp, chia sẻ dữ liệu đáp ứng tiêu chí quy định tại khoản 3 Điều 10 Nghị định 85/2016/NĐ-CP;

vii. Có phương án phòng chống tấn công mạng cho ứng dụng web; sử dụng sản phẩm Tường lửa ứng dụng web đối với các hệ thống thông tin được quy định tại khoản 2 Điều 10 Nghị định 85/2016/NĐ-CP hoặc Hệ thống Trung tâm dữ liệu, điện toán đám mây, Định danh, xác thực điện tử, chứng thực điện tử, chữ ký số, Kết nối tích hợp, chia sẻ dữ liệu đáp ứng tiêu chí quy định tại khoản 3 Điều 10 Nghị định 85/2016/NĐ-CP;

viii. Có phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử; sử dụng sản phẩm Bảo đảm an toàn thông tin cho hệ thống thư điện tử;

ix. Có phương án quản lý truy cập lớp mạng; sử dụng sản phẩm Quản lý truy cập lớp mạng đối với hệ thống Mạng nội bộ, Trung tâm giám sát điều hành an toàn thông tin mạng, đáp ứng tiêu chí quy định tại khoản 3 Điều 10 Nghị định 85/2016/NĐ-CP;

x. Có phương án giám sát hệ thống thông tin tập trung sử dụng sản phẩm Giám sát hệ thống thông tin tập trung;

xi. Có phương án giám sát an toàn hệ thống thông tin tập trung sử dụng sản phẩm Quản lý và phân tích sự kiện an toàn thông tin hoặc sản phẩm tương đương;

xii. Có phương án quản lý sao lưu dự phòng tập trung sử dụng hệ thống lưu trữ tập trung và sản phẩm quản lý lưu trữ tập trung;

xiii. Có phương án quản lý phần mềm phòng chống mã độc trên máy chủ/máy tính người dùng, sử dụng sản phẩm Phòng, chống mã độc và/hoặc sản phẩm Phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu cuối, có chức năng quản lý tập trung;

xiv. Có phương án phòng, chống thất thoát dữ liệu; sử dụng sản phẩm Phòng, chống thất thoát dữ liệu đối với hệ thống thông tin có xử lý thông tin bí mật nhà nước hoặc hệ thống Cơ sở dữ liệu dùng chung đáp ứng tiêu chí quy định tại khoản 3 Điều 10 Nghị định 85/2016/NĐ-CP;

xv. Có phương án dự phòng kết nối mạng Internet cho các máy chủ dịch vụ;

xvi. Có phương án bảo đảm an toàn cho mạng không dây (nếu có);

xvii. Có phương án quản lý tài khoản đặc quyền, sử dụng sản phẩm Quản lý tài khoản đặc quyền.

2. Yêu cầu về thiết lập, cấu hình hệ thống

STT	Yêu cầu	TCVN 11930:2017
1.1	**Bảo đảm an toàn mạng**	**Mục 8.2.1**
1.1.1	Kiểm soát truy cập từ bên ngoài mạng	Mục 8.2.1.2
1.1.2	Kiểm soát truy cập từ bên trong mạng	Mục 8.2.1.3
1.1.3	Nhật kí hệ thống	Mục 8.2.1.4
1.1.4	Phòng chống xâm nhập	Mục 8.2.1.5
1.1.5	Phòng chống phần mềm độc hại trên môi trường mạng	Mục 8.2.1.6
1.1.6	Bảo vệ thiết bị hệ thống	Mục 8.2.1.7
1.2	**Bảo đảm an toàn máy chủ**	**Mục 8.2.2**
1.2.1	Xác thực	Mục 8.2.2.1
1.2.2	Kiểm soát truy cập	Mục 8.2.2.2
1.2.3	Nhật ký hệ thống	Mục 8.2.2.3
1.2.4	Phòng chống xâm nhập	Mục 8.2.2.4
1.2.5	Phòng chống phần mềm độc hại	Mục 8.2.2.5
1.2.6	Xử lý máy chủ khi chuyển giao	Mục 8.2.2.6
1.3	**Bảo đảm an toàn ứng dụng**	**Mục 8.2.3**
1.3.1	Xác thực	Mục 8.2.3.1
1.3.2	Kiểm soát truy cập	Mục 8.2.3.2
1.3.3	Nhật kí hệ thống	Mục 8.2.3.3
1.3.4	Bảo mật thông tin liên lạc	Mục 8.2.3.4
1.3.5	Chống chối bỏ	Mục 8.2.3.5
1.3.6	An toàn ứng dụng và mã nguồn	Mục 8.2.3.6
1.4	**Bảo đảm an toàn dữ liệu**	**Mục 8.2.4**
1.4.1	Nguyên vẹn dữ liệu	Mục 8.2.4.1
1.4.2	Bảo mật dữ liệu	Mục 8.2.4.2
1.4.3	Sao lưu dự phòng	Mục 8.2.4.3

Phụ lục V
YÊU CẦU CƠ BẢN BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN ĐỐI VỚI HỆ THỐNG THÔNG TIN CẤP ĐỘ 5

(Ban hành kèm theo Thông tư số 12 /2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ trưởng Bộ Thông tin và Truyền thông)

I. YÊU CẦU QUẢN LÝ

STT	Yêu cầu	TCVN 11930:2017
1.1	**Thiết lập chính sách an toàn thông tin**	**Mục 9.1.1**
1.1.1	Chính sách an toàn thông tin	Mục 9.1.1.1
1.1.2	Xây dựng và công bố	Mục 9.1.1.2
1.1.3	Rà soát, sửa đổi	Mục 9.1.1.3
1.2	**Tổ chức bảo đảm an toàn thông tin**	**Mục 9.1.2**
1.2.1	Đơn vị chuyên trách về an toàn thông tin	Mục 9.1.2.1
1.2.2	Phối hợp với cơ quan/tổ chức có thẩm quyền	Mục 9.1.2.2
1.3	**Bảo đảm nguồn nhân lực**	**Mục 9.1.3**
1.3.1	Tuyển dụng	Mục 9.1.3.1
1.3.2	Trong quá trình làm việc	Mục 9.1.3.2
1.3.3	Chấm dứt hoặc thay đổi công việc	Mục 9.1.3.3
1.4	**Quản lý thiết kế, xây dựng hệ thống**	**Mục 9.1.4**
1.4.1	Thiết kế an toàn hệ thống thông tin	Mục 9.1.4.1
1.4.2	Phát triển phần mềm thuê khoán	Mục 9.1.4.2
1.4.3	Thử nghiệm và nghiệm thu hệ thống	Mục 9.1.4.3
1.5	**Quản lý vận hành hệ thống**	**Mục 9.1.5**
1.5.1	Quản lý an toàn mạng	Mục 9.1.5.1
1.5.2	Quản lý an toàn máy chủ và ứng dụng	Mục 9.1.5.2
1.5.3	Quản lý an toàn dữ liệu	Mục 9.1.5.3
1.5.4	Quản lý an toàn thiết bị đầu cuối	Mục 9.1.5.4
1.5.5	Quản lý phòng chống phần mềm độc hại	Mục 9.1.5.5
1.5.6	Quản lý giám sát an toàn hệ thống thông tin	Mục 9.1.5.6
1.5.7	Quản lý điểm yếu an toàn thông tin	Mục 9.1.5.7
1.5.8	Quản lý sự cố an toàn thông tin	Mục 9.1.5.8
1.5.9	Quản lý an toàn người sử dụng đầu cuối	Mục 9.1.5.9

1.6	**Phương án Quản lý rủi ro an toàn thông tin**
1.7	**Phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ**

II. YÊU CẦU KỸ THUẬT

1. Yêu cầu về thiết kế hệ thống

a) Thiết kế các vùng mạng trong hệ thống theo chức năng, các vùng mạng tối thiểu bao gồm:

i. Vùng mạng nội bộ;

ii. Vùng mạng biên;

iii. Vùng DMZ;

iv. Vùng máy chủ nội bộ;

v. Vùng mạng không dây (nếu có) tách riêng, độc lập với các vùng mạng khác;

vi. Vùng mạng máy chủ cơ sở dữ liệu;

vii. Vùng quản trị;

viii. Vùng quản trị thiết bị hệ thống.

b) Có phương án thiết kế bảo đảm các yêu cầu sau:

i. Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn sử dụng sản phẩm Mạng riêng ảo;

ii. Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập, sử dụng sản phẩm Phòng, chống xâm nhập lớp mạng;

iii. Có phương án cân bằng tải, dự phòng nóng cho các thiết bị mạng;

iv. Có phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu; sử dụng sản phẩm Tường lửa cơ sở dữ liệu đối với hệ thống thông tin được quy định tại khoản 2 Điều 11 Nghị định 85/2016/NĐ-CP;

v. Có phương án chặn lọc phần mềm độc hại trên môi trường mạng sử dụng sản phẩm Tường lửa tích hợp chức năng phòng, chống mã độc trên môi trường mạng hoặc phương án tương đương;

vi. Có phương án phòng chống tấn công từ chối dịch vụ; sử dụng dịch vụ của doanh nghiệp hoặc sản phẩm Phòng, chống tấn công từ chối dịch vụ đối với các hệ thống thông tin được quy định tại khoản 2, khoản 3 Điều 11 Nghị định 85/2016/NĐ-CP;

vii. Có phương án phòng chống tấn công mạng cho ứng dụng web; sử dụng sản phẩm Tường lửa ứng dụng web đối với hệ thống thông tin theo quy định tại khoản 2 Điều 11 Nghị định 85/2016/NĐ-CP;

viii. Có phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử, sử dụng sản phẩm Bảo đảm an toàn thông tin cho hệ thống thư điện tử;

ix. Có phương án quản lý truy cập lớp mạng, sử dụng sản phẩm Quản lý truy cập lớp mạng;

x. Có phương án giám sát hệ thống thông tin tập trung sử dụng sản phẩm Giám sát hệ thống thông tin tập trung;

xi. Có phương án giám sát an toàn hệ thống thông tin tập trung sử dụng sản phẩm Quản lý và phân tích sự kiện an toàn thông tin hoặc sản phẩm tương đương;

xii. Có phương án quản lý sao lưu dự phòng tập trung sử dụng hệ thống lưu trữ tập trung và sản phẩm quản lý lưu trữ tập trung;

xiii. Có phương án quản lý phần mềm phòng chống mã độc trên máy chủ/máy tính người dùng, sử dụng sản phẩm Phòng, chống mã độc và/hoặc sản phẩm Phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu cuối, có chức năng quản lý tập trung;

xiv. Có phương án phòng, chống thất thoát dữ liệu; sử dụng sản phẩm Phòng, chống thất thoát dữ liệu đối với hệ thống thông tin có xử lý thông tin bí mật nhà nước hoặc hệ thống thông tin quy định tại khoản 2 Điều 11 Nghị định 85/2016/NĐ-CP;

xv. Có phương án dự phòng kết nối mạng Internet cho các máy chủ dịch vụ;

xvi. Có phương án bảo đảm an toàn cho mạng không dây (nếu có);

xvii. Có phương án quản lý tài khoản đặc quyền, sử dụng sản phẩm Quản lý tài khoản đặc quyền;

xviii. Có phương án dự phòng hệ thống ở vị trí địa lý khác nhau, cách nhau tối thiểu 30 km;

xix. Có phương án dự phòng cho kết nối mạng giữa các hệ thống chính và dự phòng.

2. Yêu cầu về thiết lập, cấu hình hệ thống

STT	Yêu cầu	TCVN 11930:2017
1.1	**Bảo đảm an toàn mạng**	**Mục 9.2.1**
1.1.1	Kiểm soát truy cập từ bên ngoài mạng	Mục 9.2.1.2
1.1.2	Kiểm soát truy cập từ bên trong mạng	Mục 9.2.1.3
1.1.3	Nhật kí hệ thống	Mục 9.2.1.4
1.1.4	Phòng chống xâm nhập	Mục 9.2.1.5

1.1.5	Phòng chống phần mềm độc hại trên môi trường mạng	Mục 9.2.1.6
1.1.6	Bảo vệ thiết bị hệ thống	Mục 9.2.1.7
1.2	**Bảo đảm an toàn máy chủ**	**Mục 9.2.2**
1.2.1	Xác thực	Mục 9.2.2.1
1.2.2	Kiểm soát truy cập	Mục 9.2.2.2
1.2.3	Nhật ký hệ thống	Mục 9.2.2.3
1.2.4	Phòng chống xâm nhập	Mục 9.2.2.4
1.2.5	Phòng chống phần mềm độc hại	Mục 9.2.2.5
1.2.6	Xử lý máy chủ khi chuyển giao	Mục 9.2.2.6
1.3	**Bảo đảm an toàn ứng dụng**	**Mục 9.2.3**
1.3.1	Xác thực	Mục 9.2.3.1
1.3.2	Kiểm soát truy cập	Mục 9.2.3.2
1.3.3	Nhật kí hệ thống	Mục 9.2.3.3
1.3.4	Bảo mật thông tin liên lạc	Mục 9.2.3.4
1.3.5	Chống chối bỏ	Mục 9.2.3.5
1.3.6	An toàn ứng dụng và mã nguồn	Mục 9.2.3.6
1.4	**Bảo đảm an toàn dữ liệu**	**Mục 9.2.4**
1.4.1	Nguyên vẹn dữ liệu	Mục 9.2.4.1
1.4.2	Bảo mật dữ liệu	Mục 9.2.4.2
1.4.3	Sao lưu dự phòng	Mục 9.2.4.3