BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
	Độc lập - Tự do - Hạnh phúc
Số: /2017/TT - BTTTT	*Hà Nội, ngày tháng năm 2017*

THÔNG TƯ
Quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP 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 132/2013/NĐ-CP ngày 16 tháng 10 năm 2013 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Thông tin và Truyền thông;

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;

Bộ trưởng Bộ Thông tin và Truyền thông ban hành Thông tư hướng dẫn 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: Hướng dẫn xác định cấp độ; 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, chia sẻ thông tin.

Hệ thống thông tin phục vụ hoạt động quốc phòng, an ninh do Bộ Quốc phòng, Bộ Công an quản lý không thuộc phạm vi điều chỉnh của Thông tư này.

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.

Chương II
HƯỚNG DẪN XÁC ĐỊNH HỆ THỐNG THÔNG TIN

Điều 3. Xác định hệ thống thông tin

1. 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.

2. Hệ thống thông tin có thể hoạt động độc lập, được thiết lập nhằm trực tiếp phục vụ hoặc hỗ trợ hoạt động nghiệp vụ, sản xuất, kinh doanh cụ thể của cơ quan, tổ chức.

3. Hệ thống thông tin được thiết lập, hình thành thông qua một hoặc một số hình thức sau:

a) Đầu tư xây dựng, thiết lập mới;

b) Nâng cấp, mở rộng, tích hợp một hoặc một số hệ thống đã có;

c) Thuê hoặc chuyển giao hệ thống.

4. Việc xác định hệ thống thông tin để xác định cấp độ gắn liền với việc xác định chủ quản hệ thống thông tin. Mỗi hệ thống thông tin chỉ có một chủ quản hệ thống thông tin.

Điều 4. Phân loại hệ thống thông tin

Hệ thống thông tin được phân loại theo chức năng phục vụ hoạt động nghiệp vụ như sau:

1. 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.

Hệ thống thông tin phục vụ hoạt động nội bộ bao gồm nhưng không bị giới hạn bởi các loại hình hệ thống như sau:

a) Hệ thống thư điện tử nội bộ;

b) Hệ thống quản lý văn bản và điều hành nội bộ;

c) Hệ thống họp, hội nghị truyền hình trực tuyến;

d) Hệ thống quản lý thông tin cụ thể (nhân sự, tài chính, tài sản hoặc lĩnh vực chuyên môn nghiệp vụ cụ thể khác) hoặc hệ thống quản lý thông tin tổng thể (tích hợp quản lý nhiều chức năng, nghiệp vụ khác nhau);

đ) Hệ thống xử lý thông tin nội bộ.

2. 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 lĩnh vực chuyên ngành khác.

Hệ thống thông tin phục vụ người dân, doanh nghiệp bao gồm nhưng không bị giới hạn bởi các loại hình hệ thống như sau:

a) Hệ thống thư điện tử công cộng;

b) Hệ thống quản lý văn bản và điều hành công cộng;

c) Hệ thống một cửa điện tử;

d) Hệ thống trang, cổng thông tin điện tử;

đ) Hệ thống cung cấp hoặc hỗ trợ cung cấp dịch vụ trực tuyến;

e) Hệ thống chăm sóc khách hàng.

3. 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.

Hệ thống cơ sở hạ tầng thông tin bao gồm nhưng không bị giới hạn bởi các loại hình hệ thống sau:

a) Mạng nội bộ, mạng diện rộng, mạng truyền số liệu chuyên dùng;

b) Hệ thống cơ sở dữ liệu, trung tâm dữ liệu, điện toán đám mây;

c) Hệ thống xác thực điện tử, chứng thực điện tử, chữ ký số;

d) Hệ thống kết nối liên thông, trục tích hợp các hệ thống thông tin.

4. 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.

Hệ thống thông tin điều khiển công nghiệp bao gồm nhưng không bị giới hạn bởi các loại hình hệ thống sau:

a) Hệ thống điều khiển lập trình được (PLCs);

b) Hệ thống điều khiển phân tán (DCS);

c) Hệ thống giám sát và thu thập dữ liệu (SCADA).

5. Hệ thống thông tin khác là hệ thống thông tin không thuộc các loại hình trên, 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.

Điều 5. Chủ quản hệ thống thông tin

1. Chủ quản hệ thống thông tin là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin.

2. Đối với cơ quan, tổ chức nhà nước, 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;

3. Đối với doanh nghiệp và tổ chức khác, chủ quản hệ thống thông tin là cấp có thẩm quyền quyết định đầu tư dự án xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin.

4. Chủ quản hệ thống thông tin có thể ủy quyền cho một tổ chức thay mặt mình thực hiện quyền quản lý trực tiếp đối với hệ thống thông tin và trách nhiệm bảo đảm an toàn hệ thống thông tin theo quy định của pháp luật. Tổ chức được ủy quyền phải trực tiếp thực hiện quyền và nghĩa vụ của chủ quản hệ thống thông tin mà không được ủy quyền lại cho bên thứ ba.

Điều 6. 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 vân hành hệ thống thông tin.

2. Trong trường hợp hệ thống thông tin lớn hoặc phân tán, có nhiều hơn một đơn vị vận hành hệ thống thông tin, chủ quản hệ thống thông tin chỉ định một đơn vị làm đầu mối để 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 chủ quản hệ thống thông tin thuê ngoài dịch vụ công nghệ thông tin, đơn vị vận hành hệ thống thông tin là bên cung cấp dịch vụ.

Điều 7. Xác định cấp độ an toàn hệ thống thông tin

Việc xác định cấp độ an toàn hệ thống thông tin thực hiện như sau:

1. Xác định và phân loại hệ thống thông tin, xác định chủ quản hệ thống thông tin, đơn vị vận hành hệ thống thông tin căn cứ theo quy định tại Điều 5, Điều 6 Nghị định số 85/2016/NĐ-CP và các Điều 3,4,5,6 Thông tư này.

2. Xác định loại thông tin được xử lý thông qua hệ thống thông tin căn cứ theo quy định tại khoản 1 Điều 6 Nghị định số 85/2016/NĐ-CP.

3. Xác định cấp độ căn cứ theo quy định tại các điều từ Điều 7 đến Điều 11 Nghị định số 85/2016/NĐ-CP.4. Đối với hệ thống thông tin đề xuất là cấp độ 4 hoặc cấp độ 5, thuyết minh đề xuất cấp độ làm rõ nội dung sau đây:

a) Xác định 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;

b) Thuyết minh về mức độ đặc biệt quan trọng của loại hình thông tin, dữ liệu được xử lý hoặc lưu trữ trên hệ thống (nếu có);

c) Đánh giá khái quát về nguy cơ và mức độ rủi ro về an toàn thông tin mạng đối với các hệ thống đã được xác định;

d) 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 từng hệ thống đã được xác định. Trên cơ sở đó, thuyết minh yêu cầu cần phải vận hành 24/7 và không chấp nhận ngừng vận hành mà không có kế hoạch trước.

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

Điều 8. 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; tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin và tiêu chuẩn, quy chuẩn kỹ thuật chuyên ngành có liên quan khác.

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

3. Yêu cầu cơ bản bao gồm:

a) Yêu cầu kỹ thuật: An toàn hạ tầng mạng; an toàn máy chủ; an toàn ứng dụng và an toàn dữ liệu;

b) Yêu cầu quản lý: Chính sách chung; tổ chức, nhân sự; quản lý thiết kế, xây dựng; quản lý vận hành; kiểm tra, đánh giá và quản lý rủi ro.

4. 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 số 85/2016/NĐ-CP, cụ thể như sau:

a) Đối với hệ thống thông tin từ cấp độ 3 trở xuống: Phương án bảo đảm an toàn thông tin phải xem xét yếu tố dùng chung giữa các hệ thống thông tin để sử dụng chung giải pháp bảo vệ, chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư thừa, trùng lặp. Trong trường hợp đầu tư mới, phải có thuyết minh về việc giải pháp đã có không đáp ứng được yêu cầu cơ bản;

b) Đối với hệ thống thông tin từ cấp độ 4 trở lên: Phương án bảo đảm an toàn thông tin cần được thiết kế đảm bảo tính sẵn sàng, phân tách và hạn chế ảnh hưởng khi một thành phần trong hệ thống hoặc có liên quan tới hệ thống bị mất an toàn thông tin.

Điều 9. Yêu cầu cơ bản đối với cấp độ 1

Phương án bảo đảm an toàn hệ thống thông tin cấp độ 1 phải đáp ứng yêu cầu sau đây:

1. Yêu cầu kỹ thuật

a) An toàn máy chủ

- Có xác thực bằng cơ chế mật khẩu và ghi nhật ký hệ thống đối với hoạt động truy nhập, quản trị máy chủ;

- Việc quản trị máy chủ từ xa sử dụng kết nối mạng có mã hoá;

b) An toàn ứng dụng

- Có xác thực bằng cơ chế mật khẩu và ghi nhật ký đối với hoạt động truy cập ứng dụng và đăng nhập chức năng quản trị;

c) An toàn dữ liệu

- Dữ liệu trên hệ thống được định kỳ sao lưu dự phòng tùy theo yêu cầu, mục đích sử dụng.

2. Yêu cầu quản lý:

a) Chính sách chung: Có chính sách an toàn thông tin cho đối tượng quản trị, vận hành hệ thống;

b) Tổ chức, nhân sự: Có đầu mối liên hệ để thông báo, trao đổi, xử lý vấn đề phát sinh hoặc sự cố mất an toàn thông tin trong hệ thống.

Điều 10. Yêu cầu cơ bản đối với cấp độ 2

Phương án bảo đảm an toàn hệ thống thông tin cấp độ 2 phải đáp ứng yêu cầu như đối với cấp độ 1 và bổ sung yêu cầu sau đây:

1. Yêu cầu kỹ thuật

a) An toàn hạ tầng mạng

- Hạ tầng mạng được phân vùng thành từng vùng mạng khác nhau theo yêu cầu, mục đích sử dụng;

- Có phương án sử dụng tường lửa bảo vệ để ngăn chặn truy cập bất hợp pháp giữa các vùng mạng với mạng Internet;

- Có cơ chế xác thực và mã hoá khi sử dụng mạng không dây (nếu có);

- Có phương án xác thực người quản trị trên các thiết bị mạng quan trọng;

- Có phương án quản trị các thiết bị từ xa (nếu có) thông qua các giao thức hỗ trợ mã hoá.

b) An toàn máy chủ

- Có sử dụng phần mềm phòng chống mã độc trên máy chủ và có cơ chế tự động cập nhật phiên bản mới hoặc dấu hiệu nhận dạng mã độc mới cho phần mềm này;

- Có xác thực bằng cơ chế mật khẩu đảm bảo độ phức tạp, yêu cầu thay đổi định kỳ theo quy định của tổ chức và có cơ chế phòng chống dò quét mật khẩu. Các thông tin xác thực được lưu trên hệ thống dưới dạng mã hoá;

- Có phương án vô hiệu hoá các tài khoản mặc định hoặc không hoạt động trên hệ thống; vô hiệu hoá các dịch vụ, phần mềm không sử dụng trên máy chủ;

- Có ghi nhật ký hệ thống đối với hoạt động truy nhập, quản trị máy chủ;

- Có thiết lập cơ chế cập nhật bản vá điểm yếu an toàn thông tin cho hệ điều hành và các dịch vụ hệ thống trên máy chủ;

c) An toàn ứng dụng

- Có thiết lập yêu cầu bảo đảm mật khẩu trên ứng dụng đủ độ phức tạp để phòng chống được tấn công dò quét mật khẩu; các thông tin xác thực được lưu dưới dạng mã hoá;

- Có thiết lập yêu cầu ghi nhật ký truy cập, lỗi phát sinh;

- Có sử dụng kết nối mạng có mã hoá trong việc quản trị ứng dụng từ xa;

d) An toàn dữ liệu

Có phương án sử dụng hệ thống hoặc phương tiện lưu trữ độc lập để sao lưu dự phòng các dữ liệu quan trọng trên máy chủ. Việc sao lưu được thực hiện định kỳ theo quy định của tổ chức.

2. Yêu cầu quản lý

a) Chính sách chung

- Có chính sách an toàn thông tin cho người sử dụng bao gồm nhưng không giới hạn bởi các chính sách truy nhập và sử dụng mạng và tài nguyên trên Internet; truy nhập và sử dụng ứng dụng;

- Có chính sách an toàn thông tin cho người quản trị, vận hành hệ thống bao gồm nhưng không giới hạn bởi chính sách quản lý an toàn hạ tầng mạng, an toàn máy chủ, an toàn ứng dụng và an toàn dữ liệu;

b) Tổ chức, nhân sự

Có quy trình, thủ tục để cấp phát, loại bỏ tài khoản, quyền truy cập của cán bộ mới tham gia sử dụng hệ thống hoặc cán bộ ngừng sử dụng hệ thống;

c) Quản lý thiết kế, xây dựng

- Có tài liệu thiết kế, mô tả về các biện pháp bảo đảm an toàn hệ thống thông tin;

- Có phương án kiểm tra, xác minh hệ thống được triển khai tuân thủ theo đúng tài liệu thiết kế và yêu cầu bảo đảm an toàn thông tin trước khi nghiệm thu, bàn giao;

- Có hồ sơ đề xuất cấp độ được thẩm định, phê duyệt bởi đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin;

d) Quản lý vận hành

- Có quy trình quản lý vận hành hệ thống phù hợp yêu cầu kỹ thuật cơ bản; quản lý sự thay đổi, di chuyển hệ thống; kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống;

- Có phương án ứng cứu sự cố trong tình huống xảy ra sự cố an toàn thông tin.

đ) Kiểm tra, đánh giá và quản lý rủi ro

- Có phương án định kỳ 02 năm hoặc đột xuất khi cần thiết thực hiện kiểm tra, đánh giá an toàn thông tin và đánh giá rủi ro an toàn thông tin;

- Việc kiểm tra, đánh giá an toàn thông tin và đánh giá rủi ro được thực hiện bởi đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin thực hiện hoặc thuê ngoài.

Điều 11. Yêu cầu cơ bản đối với cấp độ 3

Phương án bảo đảm an toàn hệ thống thông tin cấp độ 3 phải đáp ứng yêu cầu như đối với cấp độ 2 và bổ sung yêu cầu sau đây:

1. Yêu cầu kỹ thuật

a) An toàn hạ tầng mạng

- Có thiết kế vùng mạng dành riêng bao gồm vùng mạng riêng cho máy chủ nội bộ, vùng mạng riêng cho các máy chủ cung cấp các dịch vụ hệ thống cần thiết (như dịch vụ DNS, DHCP, NTP và các dịch vụ khác), vùng mạng riêng máy chủ cơ sở dữ liệu và các vùng mạng riêng khác theo yêu cầu của tổ chức;

- Có thiết kế vùng mạng nội bộ thành các mạng chức năng riêng theo yêu cầu nghiệp vụ; phân vùng mạng riêng cho mạng không dây tách biệt với các vùng mạng chức năng;

- Có phương án cân bằng tải và giảm thiểu tấn công từ chối dịch vụ;

- Có thiết kế hệ thống quản lý lưu trữ tập trung và giám sát an toàn thông tin;

- Có phương án sử dụng tường lửa giữa các vùng mạng quan trọng;

- Có phương án phát hiện, phòng chống xâm nhập và chặn lọc phần mềm độc hại giữa mạng Internet và các mạng bên trong;

- Lưu trữ nhật ký các thiết bị mạng và quản lý tập trung trong vùng mạng quản trị. Nhật ký của các thiết bị mạng cần lưu trữ tối thiểu trong 03 tháng;

- Có thiết kế dự phòng cho các thiết bị mạng chính trong hệ thống đảm bảo duy trì hoạt động bình thường của hệ thống khi một thiết bị mạng gặp sự cố;

- Có phương án cập nhật phần mềm, xử lý điểm yếu an toàn thông tin và cấu hình tối ưu thiết bị mạng trước khi đưa vào sử dụng trong mạng;

- Có phương án xác thực người quản trị trên tất cả các thiết bị mạng trong đó đảm bảo yêu cầu về mật khẩu mạnh, phòng chống dò quét mật khẩu;

- Giới hạn các nguồn truy nhập, quản trị các thiết bị mạng.

- Các thiết bị mạng cho phép quản trị thông qua mạng Internet phải sử dụng mạng riêng ảo hoặc các phương pháp khác tương đương.

- Có ghi nhật ký đối với các hoạt động trên thiết bị mạng nội bộ và bảo đảm đồng bộ thời gian nhật ký với máy chủ thời gian;

- Có mã hoá thông tin xác thực lưu trên thiết bị mạng;

b) An toàn máy chủ

- Có phương án quản lý xác thực tập trung; chống đăng nhập tự động và tự động huỷ phiên đăng nhập sau một khoảng thời gian chờ phù hợp với chính sách của tổ chức;

- Có thiết lập quyền truy nhập, quản trị, sử dụng tài nguyên của từng tài khoản trên hệ thống phù hợp với nhiệm vụ, yêu cầu nghiệp vụ khác nhau;

- Có phương án quản lý bản vá, nâng cấp phần mềm trên hệ thống tập trung;

- Có phương án lưu trữ và quản lý tập trung nhật ký máy chủ. Nhật ký được lưu tối thiểu 03 tháng;

- Có phương án đồng bộ nhật ký máy chủ với hệ thống giám sát an toàn thông tin;

- Giới hạn các nguồn cho phép truy nhập, quản trị máy chủ; việc quản trị máy chủ thông qua mạng Internet phải sử dụng mạng riêng ảo hoặc các phương pháp khác tương đương;

- Sử dụng tường lửa trên từng máy chủ nhằm thiết lập chỉ cho phép các kết nối hợp pháp theo các dịch vụ được máy chủ cung cấp;

- Có phương án sao lưu dự phòng hệ điều hành máy chủ, cấu hình máy chủ phù hợp với yêu cầu của tổ chức;

- Có ghi nhật ký đối với các hoạt động truy nhập, quản trị, phát sinh lỗi;

c) An toàn ứng dụng

- Có thiết lập yêu cầu thay đổi mật khẩu định kỳ đối với tài khoản quản trị ứng dụng; giới hạn thời gian chờ để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng;

- Có thiết lập tách biệt ứng dụng quản trị với ứng dụng cung cấp dịch vụ của ứng dụng và đảm bảo ứng dụng hoạt động với quyền tối thiểu trên hệ thống;

- Giới hạn các nguồn cho phép truy nhập, quản trị ứng dụng; việc quản trị ứng dụng thông qua mạng Internet phải sử dụng mạng riêng ảo hoặc các phương pháp khác tương đương;

d) An toàn dữ liệu

- Có phương án mã hoá dữ liệu lưu trữ (không phải là thông tin, dữ liệu công khai) trên hệ thống lưu trữ/phương tiện lưu trữ;

- Có phương án tự động sao lưu dự phòng đối với thông tin/dữ liệu phù hợp với tần suất thay đổi của dữ liệu;

2. Yêu cầu quản lý

a) Chính sách chung

Định kỳ 02 năm hoặc đột xuất khi cần thiết thực hiện rà soát, cập nhật chính sách chung về an toàn thông tin;

b) Tổ chức, nhân sự

- Có kế hoạch và định kỳ tổ chức đào tạo, bồi dưỡng, tuyên truyền, phổ biến nâng cao kiến thức, kỹ năng về an toàn thông tin cho cán bộ quản lý và cán bộ kỹ thuật có liên quan;

- Có chính sách yêu cầu cán bộ liên quan khi thôi việc cần cam kết giữ bí mật thông tin liên quan đến thông tin cá nhân của khách hàng, thông tin riêng của tổ chức hoặc thông tin nhạy cảm khác;

c) Thiết kế, xây dựng hệ thống

Có hồ sơ đề xuất cấp độ được thẩm định bởi đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin;

d) Quản lý vận hành

- Có phương án giám sát an toàn thông tin cho hệ thống trong quá trình vận hành theo quy định của pháp luật;

- Có kế hoạch và định kỳ tổ chức diễn tập bảo đảm an toàn thông tin cho hệ thống; cử cán bộ tham gia vào các cuộc diễn tập quốc gia hoặc quốc tế do cơ quan chức năng triệu tập;

- Có kế hoạch khôi phục hoạt động bình thường của hệ thống trong trường hợp xảy ra sự cố hoặc thảm họa;

đ) Kiểm tra, đánh giá và quản lý rủi ro

- Định kỳ hàng năm thực hiện kiểm tra, đánh giá an toàn thông tin và đánh giá rủi ro an toàn thông tin;

- Việc kiểm tra, đánh giá an toàn thông tin và đánh giá rủi ro phải do tổ chức chuyên môn được cơ quan có thẩm quyền cấp phép hoặc tổ chức sự nghiệp

nhà nước có chức năng, nhiệm vụ phù hợp do chủ quản hệ thống thông tin chỉ định thực hiện theo quy định của pháp luật.

Điều 12. Yêu cầu cơ bản đối với cấp độ 4

Phương án bảo đảm an toàn hệ thống thông tin cấp độ 4 phải đáp ứng yêu cầu như đối với cấp độ 3 và bổ sung yêu cầu sau đây:

1. Yêu cầu về kỹ thuật

a) An toàn hạ tầng mạng

- Có phương án phát hiện phòng chống xâm nhập giữa các vùng mạng quan trọng;

- Có phương án quản lý mạng không giây (nếu có) tập trung;

- Có hệ thống quản lý phòng chống mã độc tập trung. Trong đó, hệ thống có chức năng cơ bản bao gồm: cập nhật dữ liệu, gửi cảnh báo, nhận thông tin điều khiển từ hệ thống quản lý tập trung tới các phần mềm được cài đặt trên máy chủ/máy trạm trong mạng;

- Có phương án dự phòng nóng cho các thiết bị mạng chính bảo đảm khả năng vận hành liên tục của hệ thống; năng lực của thiết bị dự phòng phải đáp ứng theo quy mô hoạt động của hệ thống;

- Đối với các thiết bị mạng quan trọng, có phương án sử dụng thêm các phương pháp xác thực đa nhân;

- Có phương án lưu trữ nhật ký độc lập và phù hợp với hoạt động của các thiết bị mạng; Dữ liệu nhật ký phải được lưu tối thiểu 06 tháng;

- Có phương án cảnh báo thời gian thực trực tiếp đến người quản trị hệ thống thông qua hệ thống giám sát khi phát hiện sự cố trên các thiết bị mạng;

- Có phương án chống thất thoát dữ liệu trong hệ thống;

- Có phương án kiểm tra tính tương thích, tác động của các bản vá, cập nhật an toàn thông tin đối với hoạt động của hệ thống;

- Có phương án cấu hình tối ưu, bảo đảm an toàn thông tin cho các thiết bị mạng, máy chủ trước khi đưa vào hoạt động trong hệ thống.

b) An toàn máy chủ

- Có phương án sử dụng cơ chế xác thực đa nhân tố khi truy nhập vào các máy chủ trong hệ thống;

- Có phương án lưu trữ nhật ký độc lập và phù hợp với hoạt động của máy chủ. Dữ liệu nhật ký phải được lưu tối thiểu 06 tháng;

- Có phương án kiểm tra tính toàn vẹn của các tệp tin hệ thống và tính toàn vẹn của các quyền đã được cấp trên các tài khoản hệ thống;

c) An toàn ứng dụng

- Có phương án sử dụng cơ chế xác thực đa nhân tố khi truy nhập vào các tài khoản quản trị của ứng dụng; có cơ chế yêu cầu người sử dụng thay đổi thông tin xác thực định kỳ;

- Có phương án lưu trữ nhật ký độc lập và phù hợp với hoạt động của ứng dụng. Dữ liệu nhật ký phải được lưu tối thiểu 06 tháng;

- Có cơ chế mã hóa thông tin xác thực của người sử dụng trước khi gửi đến ứng dụng qua môi trường mạng;

- Có cơ chế xác thực thông tin, nguồn gửi khi trao đổi thông tin trong quá trình quản trị ứng dụng (không phải là thông tin, dữ liệu công khai) qua môi trường mạng;

d) An toàn dữ liệu

- Có phương án kiểm tra tính toàn vẹn của dữ liệu và phát hiện, cảnh báo khi dữ liệu có sự thay đổi;

- Có phương án phân loại và quản lý các dữ liệu được lưu trữ theo từng loại/nhóm thông qua việc gán các nhãn khác nhau;

- Có phương án sử dụng hệ thống sao lưu dự phòng có khả năng chịu lỗi, bảo đảm dữ liệu có khả năng phục khôi phục khi xảy ra sự cố.

2. Yêu cầu quản lý

a) Chính sách chung

Định kỳ 01 năm hoặc đột xuất khi cần thiết thực hiện rà soát, cập nhật chính sách chung về an toàn thông tin;

b) Tổ chức, nhân sự

- Có chính sách thẩm tra, xác minh lý lịch của cán bộ quản lý và cán bộ kỹ thuật vận hành, chịu trách nhiệm về an toàn thông tin cho hệ thống, bảo đảm sự phù hợp về mặt chuyên môn nghiệp vụ, đạo đức nghề nghiệp và phù hợp với yêu cầu, tính chất đặc thù của công việc;

- Có kế hoạch và định kỳ hàng năm tổ chức đào tạo, bồi dưỡng, tuyên truyền, phổ biến nâng cao kiến thức, kỹ năng về an toàn thông tin cho cán bộ quản lý và cán bộ kỹ thuật có liên quan;

- Có chính sách xây dựng đội ngũ chuyên trách về an toàn thông tin và phân công lãnh đạo đơn vị trực tiếp phụ trách an toàn thông tin.

c) Thiết kế, xây dựng hệ thống

- Có hồ sơ đề xuất cấp độ được thẩm định bởi Bộ Thông tin và Truyền thông;

- Thực hiện kiểm tra, đánh giá tổng thể về an toàn thông tin của hệ thống trước khi đưa vào vận hành, khai thác;

d) Quản lý vận hành

- Có phương án giám sát an toàn thông tin riêng cho hệ thống theo quy định của pháp luật; cử cán bộ trực giám sát 24/7;

- Có kế hoạch và định kỳ hàng năm tổ chức diễn tập bảo đảm an toàn thông tin cho hệ thống;

- Có phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng theo quy định của pháp luật;

đ) Kiểm tra, đánh giá và quản lý rủi ro

- Định kỳ hàng năm thực hiện kiểm tra, đánh giá an toàn thông tin và đánh giá rủi ro an toàn thông tin;

- Việc kiểm tra, đánh giá an toàn thông tin và đánh giá rủi ro phải do tổ chức chuyên môn được cơ quan có thẩm quyền cấp phép hoặc tổ chức sự nghiệp nhà nước có chức năng, nhiệm vụ phù hợp do chủ quản hệ thống thông tin chỉ định thực hiện theo quy định của pháp luật.

Điều 13. Yêu cầu cơ bản đối với cấp độ 5

Phương án bảo đảm an toàn hệ thống thông tin cấp độ 5 phải đáp ứng yêu cầu như đối với cấp độ 4 và bổ sung yêu cầu sau đây:

1. Yêu cầu kỹ thuật

a) An toàn hạ tầng mạng

- Có hệ thống tường lửa, hệ thống phát hiện và phòng chống xâm nhập giữa các vùng mạng của hệ thống;

- Dữ liệu nhật ký của các thiết bị mạng được lưu tối thiểu 12 tháng;

- Có phương án dự phòng cho tất cả các thiết bị mạng đảm bảo hoạt động của hệ thống không bị gián đoạn;

b) An toàn máy chủ

- Có phương án sử dụng giải pháp phòng chống xâm nhập mức máy trạm đối với các máy chủ.

- Nhật ký của hệ thống phải được lưu tối thiểu 12 tháng.

c) An toàn ứng dụng

- Có phương án áp dụng cơ chế xác thực hai chiều khi trao đổi dữ liệu quan trọng qua môi trường mạng;

- Có phương án sử dụng thiết bị lưu trữ chuyên dụng để lưu trữ thông tin xác thực;

- Nhật ký của ứng dụng được lưu tối thiểu 12 tháng;

d) An toàn dữ liệu

- Có phương án sử dụng kênh vật lý riêng khi khi truyền đưa, trao đổi dữ liệu qua môi trường mạng;

- Có phương án lưu trữ dự phòng các dữ liệu trên hệ thống ở các vị trí địa lý khác nhau;

- Có phương án duy trì ít nhất 02 kết nối mạng từ hệ thống sao lưu dự phòng chính với hệ thống sao lưu dự phòng phụ.

2. Yêu cầu quản lý

a) Chính sách chung

Định kỳ 06 tháng hoặc đột xuất khi cần thiết thực hiện rà soát, cập nhật chính sách chung về an toàn thông tin;

b) Chính sách tổ chức, nhân sự

- Các vị trí công việc khác nhau phải bố trí cán bộ chuyên trách khác nhau, không được sử dụng cán bộ kiêm nhiệm;

- Các vị trí vận hành khai thác quan trọng cần bố trí ít nhất 02 cán bộ cùng tham gia thực hiện;

c) Thiết kế, xây dựng hệ thống

Sản phẩm, thiết bị được đầu tư trong hệ thống phải được kiểm định an toàn thông tin trước khi đưa vào vận hành khai thác;

d) Quản lý vận hành

Có kế hoạch và định kỳ 06 tháng tổ chức diễn tập bảo đảm an toàn thông tin cho hệ thống;

đ) Kiểm tra, đánh giá và quản lý rủi ro

- Định kỳ 06 tháng hoặc theo yêu cầu thực tế hoặc theo yêu cầu, cảnh báo của cơ quan chức năng thực hiện kiểm tra, đánh giá an toàn thông tin và đánh giá rủi ro an toàn thông tin;

- Việc kiểm tra, đánh giá an toàn thông tin và đánh giá rủi ro an toàn thông tin phải do tổ chức chuyên môn được cơ quan có thẩm quyền cấp phép hoặc tổ chức sự nghiệp nhà nước có chức năng, nhiệm vụ phù hợp do chủ quản hệ thống thông tin chỉ định thực hiện theo quy định của pháp luật.

Chương IV
KIỂM TRA, ĐÁNH GIÁ AN TOÀN THÔNG TIN

Điều 14. Hình thức kiểm tra, đánh giá

1. Hình thức kiểm tra, đánh giá an toàn thông tin bao gồm:

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

b) Đánh giá hiệu quả của biện pháp quản lý và kỹ thuật được áp dụng (Security Audit);

c) Đánh giá thử nghiệm xâm nhập hệ thống (Penenstration Testing);

2. Việc kiểm tra, đánh giá an toàn thông tin được thực hiện định kỳ hoặc đột xuất tùy tình hình thực tế, tuân thủ theo quy định của pháp luật.

Điều 15. Kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ

1. Hoạt động kiểm tra 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 việc tuân thủ quy định của pháp luật về xác định cấp độ an toàn hệ thống thông tin;

b) Kiểm tra việc tuân thủ quy định của pháp luật về thực hiện phương án bảo đảm an toàn hệ thống thông tin theo cấp độ.

2. Hoạt động kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ đối với hệ thống thông tin từ cấp độ 3 trở xuống được thực hiện định kỳ tối thiểu hai năm một lần theo kế hoạch do chủ quản hệ thống thông tin phê duyệt hoặc đột xuất khi có yêu cầu.

3. Hoạt động kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ đối với hệ thống thông tin từ cấp độ 4 trở lên được thực hiện định kỳ hàng năm theo kế hoạch do Bộ Thông tin và Truyền thông phê duyệt hoặc đột xuất khi có yêu cầu.

Điều 16. Đánh giá hiệu quả của biện pháp quản lý và kỹ thuật được áp dụng

1. Đánh giá hiệu quả của biện pháp quản lý và kỹ thuật được áp dụng là việc rà soát một cách tổng thể, xác minh mức độ hiệu quả của phương án bảo đảm an toàn thông tin theo từng tiêu chí, yêu cầu cơ bản cụ thể.

2. Việc đánh giá hiệu quả của biện pháp quản lý và kỹ thuật được áp dụng là cơ sở để tiến hành điều chỉnh phương án bảo đảm an toàn thông tin cho phù hợp với yêu cầu thực tiễn.

Điều 17. Đánh giá thử nghiệm xâm nhập hệ thống

1. Đánh giá thử nghiệm xâm nhập hệ thống là việc thực hiện dò quét, phát hiện lỗ hổng, điểm yếu của hệ thống, qua đó, thử nghiệm tấn công xâm nhập hệ thống và đánh giá nguy cơ, thiệt hại có thể có của hệ thống thông tin khi bị đối tượng tấn công xâm nhập.

2. Đánh giá thử nghiệm xâm nhập hệ thống được thực hiện trong các trường hợp sau đây:

a) Chủ quản hệ thống thông tin thực hiện định kỳ để chủ động hoàn thiện phương án tăng cường bảo đảm an toàn thông tin cho hệ thống;

b) Cơ quan chức năng có thẩm quyền thực hiện nhằm xác minh lỗ hổng, điểm yếu của hệ thống để cảnh báo cho chủ quản hệ thống thông tin;

c) Doanh nghiệp cung cấp dịch vụ kiểm tra, đánh giá an toàn thông tin mạng được chủ quản hệ thống thông tin cho phép thực hiện đánh giá thử nghiệm xâm nhập hệ thống.

3. Tổ chức thực hiện đánh giá thử nghiệm xâm nhập hệ thống có trách nhiệm:

a) Thông báo cho chủ quản hệ thống thông tin về điểm yếu an toàn thông tin phát hiện ra nhằm khắc phục, phòng tránh các sự cố an toàn thông tin;

b) Thực hiện công tác đảm bảo an toàn cho dữ liệu liên quan đến hệ thống được đánh giá, không công bố dữ liệu liên quan khi chưa được sự đồng ý của chủ quản hệ thống thông tin;

c) Việc đánh giá thử nghiệm xâm nhập hệ thống cần đảm bảo không ảnh hưởng đến hoạt đồng bình thường của hệ thống;

d) Cơ quan chức năng khi phát hiện ra điểm yếu an toàn thông tin thông qua hoạt động đánh giá cần thông báo cho chủ quản hệ thống thông tin và cơ quan quản lý nhà nước về an toàn thông tin để phối hợp khắc phục.

Chương V

CHẾ ĐỘ BÁO CÁO, CHIA SẺ THÔNG TIN

Điều 18. Chế độ báo cáo

1. Chủ quản hệ thống thông tin từ cấp độ 4 và 5 có thực hiện chế độ báo cáo định kỳ mỗi năm một lần và báo cáo đột xuất theo yêu cầu của cơ quan quản lý nhà nước có thẩm quyền.

2. Nội dung báo cáo bao gồm các nội dung liên quan đến công tác bảo đảm an toàn thông tin tin theo cấp độ như:

a) Tiến độ triển khai, áp dụng phương án bảo đảm an toàn thông tin theo hồ sơ xác định cấp độ đã được phê duyệt;

b) Hiệu quả áp dụng phương án bảo đảm an toàn thông tin theo hồ sơ xác định cấp độ đã được phê duyệt;

c) Đề xuất thay đổi cấp độ, phương án đảm bảo an toàn thông (nếu có);

d) Nội dung khác phục vụ công tác bảo vệ hệ thông thông tin theo cấp độ.

3. Chủ quản hệ thống thông tin cấp độ 4 và 5 gửi báo cáo qua đường bưu điện hoặc trực tiếp tại Bộ Thông tin và Truyền thông (Cục An toàn thông tin)

Điều 19. Chia sẻ thông tin

1. Chủ quản hệ thống thông tin, đơn vị vận hành hệ thống thông tin hệ thống thông tin cấp 4, 5 có trách nhiệm tham gia chia sẻ thông tin với cơ quan quản lý nhà nước về an toàn thông tin đối với công tác bảo đảm an toàn thông tin. Các chủ quản hệ thống thông tin, đơn vị vận hành hệ thống thông tin khác tham gia chia sẻ thông tin trên tinh thần tự nguyện.

2. Thông tin được chia sẻ thông qua các hình thức trực tiếp, email, văn bản hoặc hệ thống chia sẻ thông tin được vận hành bởi Bộ Thông tin và Truyền thông

3. Việc chia sẻ thông tin dựa trên nguyên tắc bí mật, chọn lọc và đảm bảo lợi ích của các bên tham gia.

4. Các thông tin được chia sẻ bao gồm thông tin về nguy cơ mất an toàn thông tin, cảnh báo an toàn thông tin, sự cố an toàn thông tin, các hoạt động bảo đảm an toàn thông tin như tuyên truyền, đào tạo, diễn tập và các thông tin khác.

Chương VI
TỔ CHỨC THỰC HIỆN

Điều 20. Hiệu lực thi hành

1. Thông tư này có hiệu lực thi hành kể từ ngày tháng năm 2017.

2. Trong quá trình thực hiện Thông tư này, nếu có vướng mắc, các cơ quan, đơn vị báo cáo về Bộ Thông tin và Truyền thông để phối hợp