BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

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

Số: 478 /CATTT-ATHTTT
V/v ban hành Sổ tay Hướng dẫn tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ (Phiên bản 1.0)

Hà Nội, ngày 30 tháng 03 năm 2024

Kính gửi:

- Đơn vị chuyên trách về công nghệ thông tin/an toàn thông tin các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn, Tổng công ty nhà nước;
- Các Ngân hàng thương mại cổ phần, tổ chức tài chính;
- Hệ thống các đơn vị chuyên trách về an toàn thông tin.

Triển khai Chỉ thị số 09/CT-TTg ngày 23/2/2024 của Thủ tướng Chính phủ về việc tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ, nhằm tạo thuận lợi trong công tác triển khải bảo đảm an toàn hệ thống thông tin theo cấp độ, Cục An toàn thông tin (Bộ Thông tin và Truyền thông) ban hành *Sổ tay Hướng dẫn tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ (Phiên bản 1.0)*.

Thông qua Sổ tay, Cục An toàn thông tin hi vọng sẽ giúp các đơn vị nắm rõ hơn về các quy định, đặc biệt là quy định về xác định chủ quản hệ thống thông tin, đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin, đơn vị vận hành hệ thống thông tin và trách nhiệm của các đơn vị có liên quan trong quá trình tổ chức xây dựng, thẩm định hồ sơ đề xuất cấp độ, phê duyệt cấp độ an toàn thông tin và triển khai đầy đủ phương án bảo đảm an toàn thông tin theo hồ sơ đề xuất cấp độ đã được phê duyệt cho các hệ thống thông tin.

Sổ tay cũng được Cục An toàn thông tin cung cấp nhiều ví dụ cụ thể thông qua việc đúc kết kinh nghiệm, trả lời thắc mắc của các cơ quan, tổ chức trong thời gian qua để các cơ quan, tổ chức dễ hiểu, dễ triển khai trong thực tiễn.

Chi tiết nội dung Sổ tay xin vui lòng tải về từ Nền tảng Hỗ trợ quản lý bảo đảm an toàn hệ thống thông tin theo cấp độ do Cục An toàn thông tin triển khai tại địa chỉ https://capdo.ais.gov.vn hoặc trên Cổng Thông tin điện tử của Cục An toàn thông tin tại địa chỉ: https://ais.gov.vn.

Hy vọng Sổ tay sẽ là tài liệu hữu ích giúp các cơ quan, tổ chức triển khai thuận lợi công tác bảo đảm an toàn hệ thống thông tin theo cấp độ, đáp ứng các yêu cầu đề ra và hoàn thành mục tiêu theo chỉ đạo của Thủ tướng Chính phủ tại Chỉ thị số 09/CT-TTg.

Trong quá trình nghiên cứu, áp dụng, Cục An toàn thông tin rất mong nhận được góp ý của các cơ quan, tổ chức để Sổ tay tiếp tục được cập nhật, bổ sung và hoàn thiện trong các phiên bản tiếp theo.

Đầu mối liên hệ, hỗ trợ của Cục An toàn thông tin:

Ông Nguyễn Minh Dũng, Phòng An toàn hệ thống thông tin, Cục An toàn thông tin, Bộ Thông tin và Truyền thông; số điện thoại: 0914.646.840, thư điện tử: dungnm@mic.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- UBND các tỉnh, thành phố trực thuộc TW;
- Bộ trưởng (để b/c);
- Thứ trưởng Phạm Đức Long (để b/c);
- Đơn vị chuyên trách về CNTT/ATTT của: Văn phòng TW Đảng; Văn phòng Quốc hội; Văn phòng Chủ tịch nước; Tòa án nhân dân tối cao; Viện Kiểm sát nhân dân tối cao;
- Cục trưởng (để b/c);
- Phó Cục trưởng Trần Đăng Khoa;
- Lưu: VT, ATHTTT.NMD.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC AN TOÀN THÔNG TIN
BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Trần Đăng Khoa

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

SỔ TAY
HƯỚNG DẪN TUÂN THỦ QUY ĐỊNH PHÁP LUẬT VÀ TĂNG CƯỜNG BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN THEO CẤP ĐỘ

(Phiên bản 1.0)

(Ban hành theo Công văn số 478/CATTT-ATHTTT ngày 30/03/2024 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông)

Hà Nội, 2024

Mục lục

Danh mục hình vẽ

Danh mục hình bảng

Lời nói đầu

Xác định cấp độ an toàn thông tin của hệ thống thông tin để áp dụng biện pháp quản lý và kỹ thuật nhằm bảo vệ hệ thống thông tin phù hợp theo cấp độ là nhiệm vụ trọng tâm, cốt lõi nhằm bảo vệ hệ thống thông tin được quy định tại Điều 22 của Luật An toàn thông tin mạng năm 2015. Trong hơn 07 năm triển khai thi hành Luật An toàn thông tin mạng và 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, các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương đã tích cực triển khai, thường xuyên tổ chức tập huấn nâng cao nhận thức, trách nhiệm, chất lượng thực thi pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ và thực hiện bảo đảm an toàn hệ thống thông tin theo mô hình 4 lớp ở mức cơ bản, đạt được một số kết quả quan trọng. Tuy nhiên, bên cạnh những kết quả đạt được, theo số liệu Cục An toàn thông tin tổng hợp từ các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ và địa phương, còn gần 40% hệ thống thông tin chưa hoàn thành việc phê duyệt cấp độ an toàn hệ thống thông tin. Hầu hết các hệ thống thông tin được phê duyệt cấp độ an toàn thông tin chưa được triển khai đầy đủ phương án bảo đảm an toàn theo hồ sơ đề xuất cấp độ được phê duyệt. Nhiều cơ quan, đơn vị chưa hiểu đúng một số quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ dẫn đến chưa tuân thủ đầy đủ, thống nhất áp dụng các quy định, tiềm ẩn các nguy cơ mất an toàn thông tin đối với các hệ thống thông tin.

Chính vì vậy, nhằm tăng cường áp dụng một cách thống nhất, phát huy hiệu quả các quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ, hỗ trợ các bộ, ngành, địa phương và các cơ quan, tổ chức khác triển khai một cách hiệu quả Chỉ thị số 09/CT-TTg ngày 23/02/2024 của Thủ tướng Chính phủ về tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ, Cục An toàn thông tin đã biên soạn *Sổ tay Hướng dẫn tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ* với nhiều ví dụ cụ thể để các cơ quan, tổ chức dễ hiểu, dễ triển khai trong thực tiễn. Đây là tài liệu tham khảo hữu ích phục vụ tra cứu và đào tạo, tập huấn công tác bảo đảm an toàn hệ thống thông tin theo cấp độ cho các đối tượng tham gia triển khai hệ thống thông tin tại Việt Nam gồm:

- Chủ quản hệ thống thông tin;
- Đơn vị chuyên trách về an toàn hệ thống thông tin của chủ quản hệ thống thông tin;
- Đơn vị vận hành hệ thống thông tin;
- Chủ đầu tư dự án, hoạt động ứng dụng công nghệ thông tin hoặc đơn vị chủ trì thuê dịch vụ công nghệ thông tin phục vụ xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin.

Về cấu trúc, Sổ tay gồm 06 Chương, cụ thể:

- *Chương 1. Tổng quan về bảo đảm an toàn hệ thống thông tin theo cấp độ:* Cung cấp các thông tin chung về khái niệm, căn cứ pháp lý, phạm vi áp dụng, trách nhiệm quản lý nhà nước và kinh phí triển khai công tác bảo đảm an toàn hệ thống thông tin theo cấp độ;

- *Chương 2. Xác định các chủ thể có liên quan:* Tập trung hướng dẫn, làm rõ trách nhiệm và cách thức xác định các chủ thể có liên quan đến hệ thống thông tin gồm (1) chủ quản hệ thống thông tin; (2) đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin; (3) đơn vị vận hành hệ thống thông tin; (4) chủ đầu tư dự án, hoạt động ứng dụng công nghệ thông tin hoặc đơn vị chủ trì thuê dịch vụ công nghệ thông tin phục vụ xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin, với những ví dụ minh họa trong các tình huống cụ thể;

- *Chương 3. Xác định cấp độ an toàn hệ thống thông tin:* Hướng dẫn chi tiết cách thức xác định cấp độ an toàn thông tin cho các hệ thống thông tin với 04 bước cơ bản gồm: (1) xác định hệ thống thông tin; (2) phân loại thông tin; (3) phân loại hệ thống thông tin; (4) xác định cấp độ an toàn hệ thống thông tin. Bên cạnh đó, theo quy định tại khoản 7 Điều 7 Thông tư số 12/2022/TT-BTTTT, Cục An toàn thông tin 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 7 Thông tư, do đó, Chương này sẽ hướng dẫn cụ thể danh mục hệ thống thông tin đối với từng loại hình hệ thống thông tin;

- *Chương 4. Xây dựng hồ sơ đề xuất cấp độ:* Hướng dẫn chi tiết cách thức xây dựng hồ sơ đề xuất cấp độ và quy chế bảo đảm an toàn thông tin cho hệ thống thông tin;

- *Chương 5. Thẩm định, phê duyệt cấp độ an toàn hệ thống thông tin:* Hướng dẫn chi tiết các nội dung có liên quan đến quy trình thẩm định hồ sơ đề xuất cấp độ và phê duyệt cấp độ an toàn hệ thống thông tin. Đặc biệt, sẽ thống nhất hướng dẫn đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin cụ thể các nội dung cần thuyết minh, làm rõ khi cho ý kiến thẩm định hồ sơ đề xuất cấp độ;

- *Chương 6. Chế độ báo cáo:* Hướng dẫn chi tiết về chế độ báo cáo trong lĩnh vực bảo đảm an toàn hệ thống thông tin theo cấp độ.

Trong quá trình nghiên cứu, áp dụng, Cục An toàn thông tin rất mong nhận được góp ý của các cơ quan, tổ chức để Sổ tay tiếp tục được cập nhật, bổ sung và hoàn thiện trong các phiên bản tiếp theo.

* Đầu mối liên hệ, hỗ trợ của Cục An toàn thông tin:

Ông Nguyễn Minh Dũng, Phòng An toàn hệ thống thông tin, Cục An toàn thông tin, Bộ Thông tin và Truyền thông; số điện thoại: 0914.646.840, thư điện tử: dungnm@mic.gov.vn./.

Hà Nội, tháng 03 năm 2024.

Chương 1.
Tổng quan về bảo đảm an toàn hệ thống thông tin theo cấp độ

1. Bảo đảm an toàn hệ thống thông tin theo cấp độ là gì?

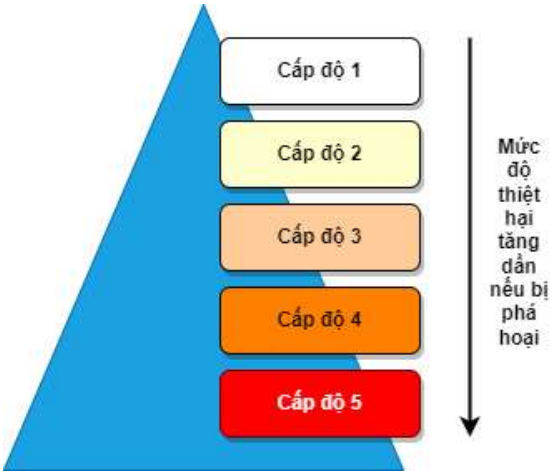
1.1. Khái niệm

Bảo đảm an toàn hệ thống thông tin theo cấp độ là các hoạt động **xác định cấp độ**, *xây dựng*, thẩm định hồ sơ đề xuất cấp độ, ***phê duyệt cấp độ an toàn thông tin*** cho các hệ thống thông tin và ***triển khai đầy đủ phương án bảo đảm an toàn hệ thống thông tin*** (bao gồm các biện pháp quản lý và kỹ thuật) nhằm bảo vệ hệ thống thông tin phù hợp theo cấp độ.

Bảo đảm an toàn hệ thống thông tin theo cấp độ là biện pháp trọng tâm, cốt lõi để bảo vệ các hệ thống thông tin được quy định tại Luật An toàn thông tin mạng năm 2015.

1.2. Phân loại

Hệ thống thông tin được phân loại theo 05 cấp độ an toàn như sau[1]:



a) *Cấp độ 1* là cấp độ mà khi bị phá hoại sẽ làm tổn hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân nhưng không làm tổn hại tới lợi ích công cộng, trật tự, an toàn xã hội, quốc phòng, an ninh quốc gia;

b) *Cấp độ 2* là cấp độ mà khi bị phá hoại sẽ làm tổn hại nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc làm tổn hại tới lợi ích công cộng nhưng không làm tổn hại tới trật tự, an toàn xã hội, quốc phòng, an ninh quốc gia;

c) *Cấp độ 3* là cấp độ mà khi bị phá hoại sẽ làm tổn hại nghiêm trọng tới sản xuất, lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại tới quốc phòng, an ninh quốc gia;

d) *Cấp độ 4* là cấp độ mà khi bị phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại nghiêm trọng tới quốc phòng, an ninh quốc gia;

đ) *Cấp độ 5* là cấp độ mà khi bị phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới quốc phòng, an ninh quốc gia. Đây là cấp độ cao nhất, các hệ thống thông tin cấp độ 5 được ưu tiên nguồn lực bảo đảm an toàn thông tin.

[1] Khoản 2 Điều 21 Luật An toàn thông tin mạng năm 2015.

1.3. Mạng, hệ thống thông tin, hệ thống thông tin quan trọng quốc gia

Mạng[2] 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[3] 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.

Như vậy, để được xác định là hệ thống thông tin, một ứng dụng công nghệ thông tin nói chung sẽ bao gồm 4 thành phần cơ bản sau đây:

(1) *Phần cứng*[4] là sản phẩm thiết bị số hoàn chỉnh; cụm linh kiện; linh kiện; bộ phận của thiết bị số, cụm linh kiện, linh kiện;

(2) *Phần mềm*[5] là chương trình máy tính được mô tả bằng hệ thống ký hiệu, mã hoặc ngôn ngữ để điều khiển thiết bị số thực hiện chức năng nhất định;

(3) *Cơ sở dữ liệu*[6] là tập hợp các dữ liệu điện tử được sắp xếp, tổ chức để truy cập, khai thác, chia sẻ, quản lý và cập nhật thông qua phương tiện điện tử;

(4) *Mạng*: Phục vụ truyền đưa, trao đổi thông tin.

Hệ thống thông tin quan trọng quốc gia[7] là hệ thống thông tin mà khi bị phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới quốc phòng, an ninh quốc gia.

Căn cứ định nghĩa nêu trên và định nghĩa an toàn hệ thống thông tin cấp độ 5 được nêu tại Mục 1.2, các hệ thống thông tin quan trọng quốc gia được đồng nhất với các hệ thống thông tin cấp độ 5.

1.4. Nguyên tắc thực hiện

Nguyên tắc bảo đảm an toàn hệ thống thông tin theo cấp độ[8]:

- Việc bảo đảm an toàn hệ thống thông tin theo cấp độ trong hoạt động của cơ quan, tổ chức được thực hiện thường xuyên, liên tục từ khâu thiết kế, xây dựng, vận hành đến khi hủy bỏ; tuân thủ theo tiêu chuẩn, quy chuẩn kỹ thuật;

- Việc bảo đảm an toàn hệ thống thông tin theo cấp độ trong hoạt động của cơ quan, tổ chức 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;

- Việc phân bổ, bố trí nguồn lực để bảo đảm an toàn hệ thống thông tin thực hiện theo thứ tự ưu tiên từ cấp độ cao xuống cấp độ thấp.

---

[2] Khoản 2 Điều 3 Luật An toàn thông tin mạng năm 2015.
[3] Khoản 3 Điều 3 Luật An toàn thông tin mạng năm 2015.
[4] Khoản 10 Điều 4 Luật Công nghệ thông tin năm 2006.
[5] Khoản 12 Điều 4 Luật Công nghệ thông tin năm 2006.
[6] Khoản 10 Điều 3 Luật Giao dịch điện tử năm 2023.
[7] Khoản 4 Điều 3 Luật An toàn thông tin mạng năm 2015.
[8] Điều 4 Nghị định số 85/2016/NĐ-CP.

2. Căn cứ pháp lý và một số văn bản chỉ đạo quan trọng liên quan

2.1. Các văn bản quy phạm pháp luật chính

Các văn bản quy phạm pháp luật chính quy định về bảo đảm an toàn thông tin theo cấp độ gồm:

a) *Luật An toàn thông tin mạng* số 86/2015/QH13 do Quốc hội Việt Nam khóa 13 ban hành ngày 19/11/2015, có hiệu lực thi hành từ ngày 01/7/2016 (sau đây gọi tắt là Luật An toàn thông tin mạng):

Luật An toàn thông tin mạng quy định một số nội dung cơ bản về bảo đảm an toàn hệ thống thông tin theo cấp độ tại Mục 3. Bảo vệ hệ thống thông tin thuộc Chương II. Bảo đảm an toàn thông tin mạng, gồm 7 Điều, cụ thể: (1) Điều 21 quy định về việc phân loại cấp độ an toàn hệ thống thông tin; (2) Điều 22 quy định các nhiệm vụ bảo vệ hệ thống thông tin; (3) Điều 23 quy định về các biện pháp bảo vệ hệ thống thông tin; (4) Điều 24 quy định về giám sát an toàn hệ thống thông tin; (5) Điều 25 quy định trách nhiệm của chủ quản hệ thống thông tin; (6) Điều 26 quy định về hệ thống thông tin quan trọng quốc gia; (7) Điều 27 quy định về trách nhiệm bảo đảm an toàn thông tin mạng cho hệ thống thông tin quan trọng quốc gia.

b) *Nghị định số 85/2016/NĐ-CP* ngày 01/7/2016 của Chính phủ về bảo đảm an toàn thông tin theo cấp độ, có hiệu lực thi hành từ ngày 01/7/2016 (sau đây gọi tắt là Nghị định số 85/2016/NĐ-CP):

Nghị định này quy định chi tiết về tiêu chí, thẩm quyền, trình tự, thủ tục xác định cấp độ an toàn hệ thống thông tin và trách nhiệm bảo đảm an toàn hệ thống thông tin theo từng cấp độ. Căn cứ các quy định tại Nghị định, các cơ quan, tổ chức thuộc đối tượng áp dụng tại Điều 2 Nghị định phải thực hiện quy trình, thủ tục xác định cấp độ và phương án bảo đảm an toàn thông tin cho các hệ thống thông tin do mình quản lý. Trên cơ sở đó, căn cứ vào các quy định về quyền và trách nhiệm bảo đảm an toàn thông tin theo cấp độ tương ứng, chủ quản hệ thống thông tin và đơn vị vận hành hệ thống thông tin sẽ triển khai các biện pháp về quản lý và kỹ thuật phù hợp để thực thi công tác bảo đảm an toàn thông tin.

c) *Thông tư số 12/2022/TT-BTTTT* ngày 12/8/2022 của Bộ trưởng 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 tháng 7 năm 2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ, có hiệu lực thi hành từ ngày 01/10/2022 (sau đây gọi tắt là Thông tư số 12/2022/TT-BTTTT):

Thông tư này được ban hành, thay thế Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ trưởng Bộ Thông tin và Truyền thông, với phạm vi điều chỉnh bao gồm: (1) xác định hệ thống thông tin và thuyết minh cấp độ an toàn hệ thống thông tin; (2) yêu cầu bảo đảm an toàn hệ thống thông tin theo cấp độ; (3) kiểm tra, đánh giá an toàn thông tin; (4) chế độ báo cáo.

2.2. Tiêu chuẩn, quy chuẩn kỹ thuật

Hệ thống tiêu chuẩn, quy chuẩn kỹ thuật về bảo đảm an toàn hệ thống thông tin theo cấp độ hiện chỉ có duy nhất *Tiêu chuẩn quốc gia TCVN 11930:2017* về Công nghệ thông tin - Các kĩ thuật an toàn - Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ (sau đây gọi tắt là Tiêu chuẩn quốc gia TCVN 11930:2017), trong đó:

- Tiêu chuẩn này quy định các yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ, bao gồm hai nhóm yêu cầu quản lý và yêu cầu kỹ thuật. Nhóm các yêu cầu quản lý là cơ sở để cơ quan, tổ chức xây dựng chính sách, quy trình quản lý an toàn thông tin cho hệ thống thông tin của mình trong quá trình thiết kế, xây dựng, vận hành, khai thác và sử dụng. Nhóm yêu cầu kỹ thuật là cơ sở để cơ quan, tổ chức thiết kế, thiết lập cấu hình hệ thống trong quá trình xây dựng hệ thống thông tin;

- Cơ quan, tổ chức sau khi xác định cấp độ an toàn và phương án bảo đảm an toàn hệ thống thông tin, có thể triển khai các biện pháp bảo đảm an toàn thông tin, đáp ứng các yêu cầu cơ bản nêu tại Tiêu chuẩn này, nhằm bảo đảm an toàn hệ thống thông tin ở mức độ cơ bản theo cấp độ tương ứng.

Khoản 1 Điều 9 Thông tư số 12/2022/TT-BTTTT khẳng định "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 kĩ thuật an toàn - yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ".

2.3. Một số văn bản chỉ đạo điều hành quan trọng

Nhằm tăng cường thực thi các quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ, Bộ Thông tin và Truyền thông đã tham mưu cho Thủ tướng Chính phủ ban hành hoặc trực tiếp ban hành một số văn bản chỉ đạo điều hành quan trọng, có liên quan, cụ thể như sau:

2.3.1. Văn bản do Thủ tướng Chính phủ ban hành

a) *Quyết định số 632/QĐ-TTg* ngày 10/5/2017 của Thủ tướng Chính phủ về việc ban hành "Danh mục lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng và hệ thống thông tin quan trọng quốc gia" (sau đây gọi tắt là Quyết định số 632/QĐ-TTg):

Quyết định số 632/QĐ-TTg được ban hành nhằm thực hiện quy định tại điểm đ khoản 3 Điều 12 Nghị định số 85/2016/NĐ-CP, trong đó xác định 11 lĩnh vực quan trọng cần ưu tiên, tập trung bảo đảm an toàn thông tin mạng và các hệ thống thông tin quan trọng quốc gia, trong bối cảnh nguồn lực có hạn. Thực hiện Quyết định này, đối với mỗi lĩnh vực, cơ quan, tổ chức là chủ quản của mỗi lĩnh vực phải xây dựng các tiêu chí và thực hiện xác định danh mục hệ thống thông tin quan trọng quốc gia thuộc phạm vi quản lý. Sau khi hệ thống thông tin quan trọng quốc gia được phê duyệt, cơ quan chủ quản của hệ thống

thông tin sẽ phối hợp với Bộ Thông tin và Truyền thông và các bộ, ngành liên quan để tập trung bảo vệ.

b) *Quyết định số 964/QĐ-TTg* ngày 10/8/2022 của Thủ tướng Chính phủ phê duyệt Chiến lược an toàn, an ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030 (sau đây gọi tắt là Chiến lược an toàn, an ning mạng quốc gia):

Tại Chiến lược này, bên cạnh việc yêu cầu chủ quản các hệ thống thông tin của cơ quan nhà nước phải nghiêm túc thực hiện các quy định về bảo đảm an toàn hệ thống thông tin theo cấp độ, Thủ tướng Chính phủ yêu cầu các doanh nghiệp chủ quản nền tảng số cũng cần phải xác định cấp độ an toàn thông tin và triển khai phương án bảo đảm an toàn hệ thống thông tin theo cấp độ đối với nền tảng số.

c) *Chỉ thị số 14/CT-TTg* ngày 25/5/2018 của Thủ tướng Chính phủ về việc nâng cao năng lực phòng, chống phần mềm độc hại (sau đây gọi tắt là Chỉ thị số 14/CT-TTg năm 2018):

Thủ tướng Chính phủ yêu cầu các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương khẩn trương phân loại, xác định cấp độ an toàn hệ thống thông tin và xây dựng phương án bảo đảm an toàn hệ thống thông tin theo cấp độ phù hợp với quy định của pháp luật và tiêu chuẩn, quy chuẩn kỹ thuật. Thời hạn hoàn thành xác định hệ thống thông tin cấp độ 4, cấp độ 5: Tháng 11 năm 2018.

d) *Chỉ thị số 14/CT-TTg* ngày 07/6/2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam (sau đây gọi tắt là Chỉ thị số 14/CT-TTg năm 2019):

Chỉ thị số 14/CT-TTg năm 2019 giới thiệu mô hình 4 lớp bảo vệ an toàn hệ thống thông tin, trong đó, đối với công tác kiểm tra, đánh giá an toàn thông tin mạng cho hệ thống thông tin thuộc quyền quản lý (lớp 3): Lựa chọn tổ chức, doanh nghiệp độc lập với tổ chức, doanh nghiệp giám sát, bảo vệ để định kỳ kiểm tra, đánh giá an toàn thông tin mạng đối với hệ thống thông tin cấp độ 3 trở lên thuộc quyền quản lý hoặc kiểm tra, đánh giá đột xuất khi có yêu cầu theo quy định của pháp luật.

Bên cạnh đó, Thủ tướng Chính phủ chỉ đạo ưu tiên sử dụng sản phẩm, giải pháp, dịch vụ của doanh nghiệp trong nước đáp ứng yêu cầu về an toàn, an ninh mạng theo quy định của pháp luật đối với các hệ thống thông tin cấp độ 3 trở lên, các hệ thống thông tin phục vụ Chính phủ điện tử. Trong quá trình thẩm định, Bộ Kế hoạch và Đầu tư, Bộ Tài chính có trách nhiệm cân đối nguồn vốn cho các dự án công nghệ thông tin, bảo đảm đạt tối thiểu 10% tổng kinh phí triển khai dự án công nghệ thông tin trong trường hợp chủ đầu tư chưa có hệ thống kỹ thuật hoặc thuê dịch vụ bảo đảm an toàn thông tin mạng chuyên biệt đáp ứng được các quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ.

đ) *Chỉ thị số 18/CT-TTg* ngày 13/10/2022 của Thủ tướng Chính phủ về đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng Việt Nam (sau đây gọi tắt là Chỉ thị số 18/CT-TTg):

Thủ tướng Chính phủ chỉ đạo:

- Hoạt động ứng cứu sự cố an toàn thông tin mạng phải chuyển từ bị động sang chủ động, trong đó tổ chức diễn tập thực chiến tối thiểu 01 lần/năm đối với hệ thống thông tin cấp độ 3 trở lên nhằm đánh giá khả năng phòng ngừa xâm nhập và khả năng phát hiện kịp thời các điểm yếu về quy trình, công nghệ, con người;

- Cơ quan chủ trì 11 lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng (theo Quyết định số 632/QĐ-TTg) chú trọng hoạt động chia sẻ thông tin về các nguy cơ, sự cố mất an toàn thông tin mạng cho các cơ quan, tổ chức, doanh nghiệp quản lý, vận hành hệ thống thông tin thuộc lĩnh vực và phục vụ kịp thời, hiệu quả cho đội ứng cứu sự cố của lĩnh vực (CERT lĩnh vực).

e) *Chỉ thị số 23/CT-TTg* ngày 26/12/2022 của Thủ tướng Chính phủ về tăng cường công tác bảo đảm an toàn thông tin mạng, an ninh thông tin cho thiết bị camera giám sát (sau đây gọi tắt là Chỉ thị số 23/CT-TTg):

Thủ tướng Chính phủ chỉ đạo các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương, tập đoàn, tổng công ti nhà nước thực hiện:

- Xác định cấp độ an toàn hệ thống thông tin và triển khai phương án bảo đảm an toàn hệ thống thông tin theo cấp độ, theo quy định của pháp luật và tiêu chuẩn, quy chuẩn kỹ thuật quốc gia về an toàn hệ thống thông tin theo cấp độ khi triển khai các hệ thống thông tin có sử dụng camera giám sát;

- Thời hạn hoàn thành: Xác định và phê duyệt cấp độ an toàn hệ thống thông tin có sử dụng camera giám sát, hoàn thành chậm nhất trong tháng 3 năm 2023; triển khai đầy đủ phương án bảo đảm an toàn hệ thống thông tin theo cấp độ đối với các hệ thống thông tin có sử dụng camera giám sát đang vận hành, hoàn thành chậm nhất trong tháng 9 năm 2023.

h) *Chỉ thị số 09/CT-TTg* ngày 23/2/2024 của Thủ tướng Chính phủ về tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ (sau đây gọi tắt là Chỉ thị số 09/CT-TTg):

Chỉ thị đặt ra 02 mục tiêu với 15 nhiệm vụ, giải pháp yêu cầu các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, địa phương; các tập đoàn, tổng công ty nhà nước, ngân hàng thương mại nhà nước, Ngân hàng Phát triển Việt Nam, Ngân hàng Chính sách xã hội, Ngân hàng Hợp tác xã Việt Nam và tổ chức tín dụng, tài chính nhà nước khác trên toàn quốc phải tập trung triển khai thực hiện một cách hiệu quả, đồng bộ, cụ thể:

- 100% hệ thống thông tin đang trong quá trình thiết kế, xây dựng, nâng cấp, mở rộng trước khi đưa vào vận hành, khai thác phải được phê duyệt cấp độ

an toàn hệ thống thông tin và triển khai đầy đủ phương án bảo đảm an toàn thông tin theo hồ sơ đề xuất cấp độ được phê duyệt;

- 100% hệ thống thông tin từ cấp độ 1 đến cấp độ 5 (nếu có) đang vận hành phải được phê duyệt cấp độ an toàn hệ thống thông tin chậm nhất trong tháng 9 năm 2024 và triển khai đầy đủ phương án bảo đảm an toàn thông tin theo hồ sơ đề xuất cấp độ được phê duyệt chậm nhất trong tháng 12 năm 2024.

2.3.2. Văn bản do Bộ Thông tin và Truyền thông ban hành

a) *Văn bản số 797/BTTTT-THH* ngày 06/3/2022 hướng dẫn một số nhiệm vụ quan trọng thúc đẩy triển khai chuyển đổi số năm 2022 (sau đây gọi tắt là Văn bản số 797/BTTTT-THH):

Tại văn bản này, Bộ Thông tin và Truyền thông đề nghị các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương tổ chức phổ biến, quán triệt tới toàn bộ các tổ chức, cá nhân liên quan về hai nguyên tắc bảo đảm an toàn, an ninh mạng, cụ thể là:

- Hệ thống chưa kết luận bảo đảm an toàn, an ninh mạng chưa đưa vào sử dụng" (Nguyên tắc Security First);

- Hệ thống thử nghiệm, có dữ liệu thật thì phải tuân thủ đầy đủ quy định như hệ thống chính thức.

b) *Văn bản số 708/BTTTT-CATTT* ngày 02/3/2024 sửa đổi, thay thế nội dung về an toàn, an ninh mạng tại Công văn số 1552/BTTTT-THH (sau đây gọi tắt là Văn bản số 708/BTTTT-CATTT):

Văn bản được ban hành nhằm đồng bộ, thống nhất nội dung về hướng dẫn về an toàn, an ninh mạng tại Mục 7 Công văn số 1552/BTTTT-THH ngày 26/4/2022 của Bộ Thông tin và Truyền thông về việc hướng dẫn kỹ thuật triển khai Đề án 06 (phiên bản 1.0) với các văn bản quy phạm pháp luật hiện hành, tạo điều kiện thuận lợi cho các bộ, ngành, địa phương triển khai công tác bảo đảm an toàn, an ninh mạng.

3. Phạm vi đối tượng áp dụng quy định về bảo đảm an toàn hệ thống thông tin theo cấp độ

Căn cứ quy định tại Điều 2 Nghị định số 85/2016/NĐ-CP, việc triển khai các nhiệm vụ bảo đảm an toàn hệ thống thông tin theo cấp độ đối với các hệ thống thông tin là bắt buộc đối với:

(1) Các cơ quan, tổ chức nhà nước gồm các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương, các doanh nghiệp nhà nước theo quy định tại khoản 11 Điều 4 Luật Doanh nghiệp 2020 và các cơ quan, tổ chức nhà nước khác;

(2) Các cơ quan, doanh nghiệp, cán nhân, tổ chức khác (như ngân hàng, tổ chức tài chính, doanh nghiệp tư nhân…) có triển khai các ứng dụng công nghệ thông tin cung cấp dịch vụ trực tuyến phục vụ người dân và doanh nghiệp.

Đối với các hệ thống thông tin khác, không thuộc phạm vi nêu trên: Khuyến khích các cơ quan, tổ chức triển khai áp dụng để bảo vệ các hệ thống thông tin do mình xây dựng, quản lý, vận hành.

4. Trách nhiệm quản lý nhà nước

Nội dung và trách nhiệm quản lý nhà nước về an toàn thông tin mạng được quy định tại Chương VII Luật An toàn thông tin mạng với Điều 51. Quy định về nội dung quản lý nhà nước về an toàn thông tin mạng và Điều 52. Quy định về trách nhiệm quản lý nhà nước về an toàn thông tin mạng, trong đó:

- Chính phủ thống nhất quản lý nhà nước về an toàn thông tin mạng;

- Bộ Thông tin và Truyền thông chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về an toàn thông tin mạng.

Đối với công tác quản lý nhà nước về bảo đảm an toàn hệ thống thông tin theo cấp độ, Điều 23 Nghị định số 85/2016/NĐ-CP quy định như sau:

4.1. Trách nhiệm của Bộ Thông tin và Truyền thông

a) Thực hiện thẩm định hồ sơ đề xuất cấp độ theo thẩm quyền quy định tại điểm a khoản 3 Điều 12 Nghị định số 85/2016/NĐ-CP;

b) Xây dựng dự thảo tiêu chuẩn quốc gia, ban hành quy chuẩn kỹ thuật quốc gia về bảo đảm an toàn thông tin theo cấp độ;

c) Hướng dẫn chi tiết việc xác định hệ thống thông tin quy định tại khoản 2 Điều 6 Nghị định số 85/2016/NĐ-CP;

d) Ban hành quy định, văn bản hướng dẫn về bảo đảm an toàn hệ thống thông tin theo cấp độ; quy định về đánh giá, chứng nhận hợp chuẩn, hợp quy về bảo đảm an toàn hệ thống thông tin theo cấp độ;

đ) Hướng dẫn các cơ quan, tổ chức thực hiện đào tạo ngắn hạn, tuyên truyền, phổ biến nâng cao nhận thức và diễn tập về an toàn thông tin;

e) Quy định chi tiết về kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin trong hoạt động của cơ quan, tổ chức nhà nước, trừ trường hợp quy định tại điểm d khoản 2 và điểm d khoản 3 Điều 23 Nghị định số 85/2016/NĐ-CP (thuộc trách nhiệm của Bộ Quốc phòng và Bộ Công an);

g) Triển khai các hệ thống hạ tầng kỹ thuật tập trung quy mô quốc gia để xử lý, giảm thiểu tấn công mạng, hỗ trợ giám sát an toàn thông tin cho hệ thống thông tin cung cấp dịch vụ công trực tuyến, phát triển Chính phủ điện tử;

h) Chịu trách nhiệm hướng dẫn, kiểm tra việc thực hiện Nghị định số 85/2016/NĐ-CP.

4.2. Trách nhiệm của Bộ Quốc phòng

a) Thực hiện thẩm định phương án bảo đảm an toàn thông tin trong hồ sơ đề xuất cấp độ theo thẩm quyền được quy định tại điểm b khoản 3 Điều 12 Nghị định số 85/2016/NĐ-CP;

b) Xây dựng dự thảo tiêu chuẩn, ban hành quy chuẩn kỹ thuật, hướng dẫn về bảo đảm an toàn đối với hệ thống thông tin thuộc phạm vi quản lý;

c) Hướng dẫn về tiêu chí quy định hệ thống thông tin tại khoản 1 Điều 9, khoản 1 Điều 10 và khoản 1 Điều 11 Nghị định số 85/2016/NĐ-CP theo chức năng, nhiệm vụ được phân công;

d) Quy định chi tiết về kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin trong hoạt động của Bộ Quốc phòng.

4.3. Trách nhiệm của Bộ Công an

a) Thực hiện thẩm định phương án bảo đảm an toàn thông tin trong hồ sơ đề xuất cấp độ theo thẩm quyền được quy định tại điểm c khoản 3 Điều 12 Nghị định số 85/2016/NĐ-CP;

b) Xây dựng dự thảo tiêu chuẩn, ban hành quy chuẩn kỹ thuật, hướng dẫn về bảo đảm an toàn đối với hệ thống thông tin thuộc phạm vi quản lý;

c) Hướng dẫn về tiêu chí quy định hệ thống thông tin tại khoản 1 Điều 9, khoản 1 Điều 10 và khoản 1 Điều 11 Nghị định số 85/2016/NĐ-CP theo chức năng, nhiệm vụ được phân công;

d) Quy định chi tiết về kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin trong hoạt động của Bộ Công an.

5. Kinh phí bảo đảm an toàn hệ thống thông tin theo cấp độ

Theo quy định tại Điều 24 Nghị định số 85/2016/NĐ-CP, kinh phí thực hiện yêu cầu về an toàn thông tin theo cấp độ trong hoạt động của cơ quan, tổ chức nhà nước do Ngân sách nhà nước bảo đảm. Do đó, có thể xem xét sử dụng Ngân sách nhà nước để chi cho các hoạt động bảo đảm an toàn hệ thống thông tin theo cấp độ. Việc sử dụng kinh phí phải tuân thủ các quy định của pháp luật về ngân sách và các quy định có liên quan.

Cụ thể:

(1) Kinh phí đầu tư cho an toàn thông tin sử dụng vốn đầu tư công thực hiện theo quy định của Luật Đầu tư công. Đối với dự án đầu tư công để xây dựng mới hoặc mở rộng, nâng cấp hệ thống thông tin, kinh phí đầu tư cho an toàn thông tin theo cấp độ được bố trí trong vốn đầu tư của dự án tương ứng;

(2) Kinh phí thực hiện giám sát, đánh giá, quản lý rủi ro an toàn thông tin; đào tạo ngắn hạn, tuyên truyền, phổ biến nâng cao nhận thức, diễn tập an toàn thông tin và ứng cứu sự cố của cơ quan, tổ chức nhà nước được cân đối bố trí trong dự toán ngân sách hàng năm của cơ quan, tổ chức nhà nước đó theo phân cấp của Luật Ngân sách nhà nước;

(3) Bộ Tài chính có trách nhiệm hướng dẫn Mục chi cho công tác bảo đảm an toàn thông tin trong dự toán ngân sách, hướng dẫn quản lý và sử dụng kinh phí sự nghiệp chi cho công tác bảo đảm an toàn thông tin trong hoạt động của các cơ quan, tổ chức nhà nước. Đối với nhiệm vụ này, Bộ Tài chính đã ban

hành Thông tư số 121/2018/TT-BTC ngày 12/12/2018 quy định về lập dự toán, quản lý, sử dụng và quyết toán kinh phí để thực hiện công tác ứng cứu sự cố, bảo đảm an toàn thông tin mạng, trong đó các nội dung chi và mức chi được quy định cụ thể tại Điều 5 và Điều 6 của Thông tư;

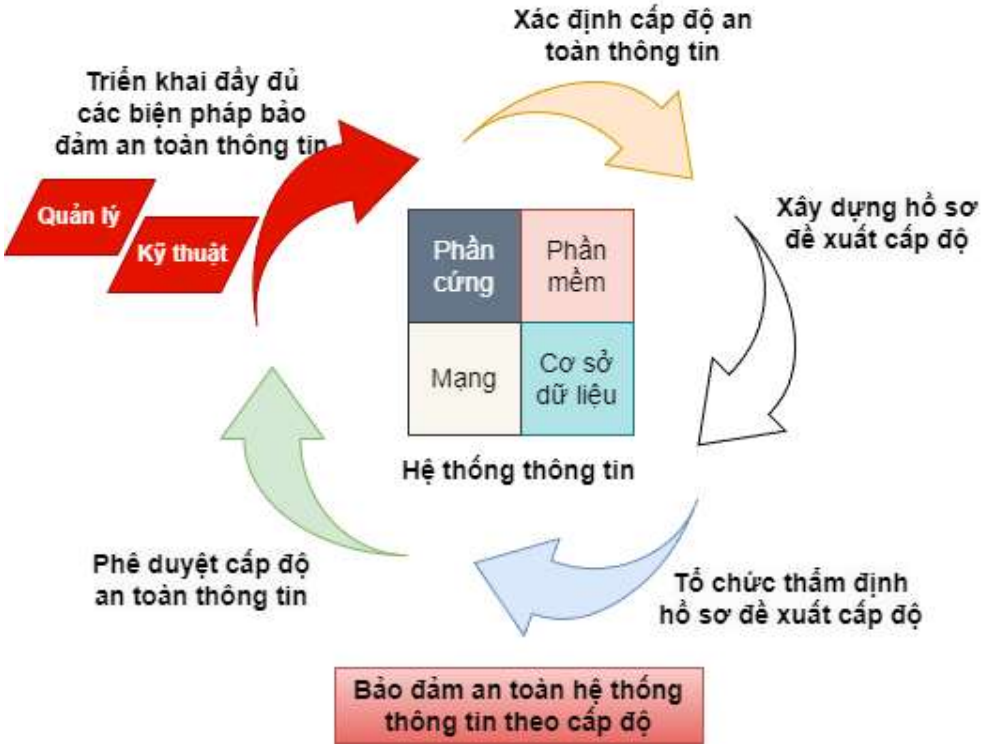
(4) Căn cứ nhiệm vụ được giao, cơ quan, tổ chức nhà nước thực hiện lập dự toán, quản lý, sử dụng và quyết toán kinh phí thực hiện nhiệm vụ bảo đảm an toàn thông tin theo quy định của Luật Ngân sách nhà nước;

(5) Tỷ lệ kinh phí chi cho hoạt động bảo đảm an toàn thông tin:

- Tại Chỉ thị số 14/CT-TTg năm 2019, Thủ tướng Chính phủ chỉ đạo: *"e) Bảo đảm tỷ lệ kinh phí chi cho các sản phẩm, dịch vụ an toàn thông tin mạng đạt* ***tối thiểu 10% trong tổng kinh phí triển khai kế hoạch ứng dụng công nghệ thông tin hàng năm, giai đoạn 5 năm và các dự án công nghệ thông tin*** *(trong trường hợp chủ đầu tư chưa có hệ thống kỹ thuật hoặc thuê dịch vụ bảo đảm an toàn thông tin mạng chuyên biệt đáp ứng được các quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ);"*;

- Tại Chiến lược an toàn, an ning mạng quốc gia, Thủ tướng Chính phủ tiếp tục chỉ đạo về đầu tư nguồn lực và bảo đảm kinh phí thực hiện: *"đ) Bố trí kinh phí chi cho an toàn, an ninh mạng đạt* ***tối thiểu 10% kinh phí chi cho khoa học công nghệ, chuyển đổi số, ứng dụng công nghệ thông tin.****"*.

TỔNG KẾT CHƯƠNG 1



Hình 1. Hoạt động bảo đảm an toàn hệ thống thông tin theo cấp độ

Chương 2.
Xác định các chủ thể có liên quan

Căn cứ nguyên tắc bảo đảm an toàn hệ thống thông tin theo cấp độ được quy định tại khoản 1 Điều 4 Nghị định số 85/2016/NĐ-CP, mỗi khi xây dựng, thiết lập mới hoặc nâng cấp, mở rộng hệ thống thông tin, các chủ thể có liên quan đến hệ thống thông tin có trách nhiệm thực hiện các quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ để bảo vệ hệ thống thông tin.

Các chủ thể có liên quan đến mỗi hệ thống thông tin bao gồm: (1) Chủ quản hệ thống thông tin; (2) Đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin; (3) Đơn vị vận hành hệ thống thông tin; (4) Chủ đầu tư dự án, hoạt động ứng dụng công nghệ thông tin hoặc đơn vị chủ trì thuê dịch vụ công nghệ thông tin phục vụ xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin.

Tuy nhiên, trong thực tiễn thời gian vừa qua, việc tổ chức triển khai hoạt động bảo đảm an toàn hệ thống thông tin theo cấp độ còn gặp nhiều khó khăn, vướng mắc do không ít cơ quan, đơn vị hiểu chưa đúng và xác định sai các chủ thể có liên quan đến hệ thống thông tin. Do đó, Chương này sẽ tập trung hướng dẫn, làm rõ trách nhiệm và cách thức xác định các chủ thể có liên quan đến hệ thống thông tin với những ví dụ minh họa trong các tình huống cụ thể.

1. Chủ quản hệ thống thông tin

1.1. Định nghĩa

Định nghĩa về chủ quản hệ thống thông tin được quy định tại khoản 5 Điều 3 Luật An toàn thông tin mạng, sau đó được làm rõ chi tiết tại khoản 1 Điều 3 Nghị định số 85/2016/NĐ-CP, cụ thể:

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.

Đối với cơ quan, tổ chức nhà nước, chủ quản hệ thống thông tin là các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương hoặc là cấp có thẩm quyền quyết định đầu tư dự án xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin đó.

1.2. Trách nhiệm của Người đứng đầu cơ quan, tổ chức là chủ quản hệ thống thông tin

Theo quy định tại khoản 1 Điều 20 Nghị định số 85/2016/NĐ-CP, Người đứng đầu của cơ quan, tổ chức là chủ quản hệ thống thông tin có trách nhiệm:

a) Trực tiếp chỉ đạo và phụ trách công tác bảo đảm an toàn thông tin trong hoạt động của cơ quan, tổ chức mình;

b) Trường hợp chưa có đơn vị chuyên trách về an toàn thông tin độc lập:

- Chỉ định đơn vị chuyên trách về công nghệ thông tin làm nhiệm vụ đơn vị chuyên trách về an toàn thông tin;

- Thành lập hoặc chỉ định bộ phận chuyên trách về an toàn thông tin trực thuộc đơn vị chuyên trách về công nghệ thông tin.

1.3. Trách nhiệm của chủ quản hệ thống thông tin

Theo quy định tại khoản 2 Điều 20 Nghị định số 85/2016/NĐ-CP, chủ quản hệ thống thông tin có trách nhiệm[9]:

a) Chỉ đạo đơn vị vận hành hệ thống thông tin lập hồ sơ đề xuất cấp độ; tổ chức thẩm định, phê duyệt hồ sơ đề xuất cấp độ;

b) Chỉ đạo, tổ chức thực hiện phương án bảo đảm an toàn hệ thống thông tin theo cấp độ đối với hệ thống thông tin thuộc phạm vi mình quản lý theo quy định tại Điều 25, 26 qvà 27 Luật An toàn thông tin mạng, Nghị định số 85/2016/NĐ-CP và quy định của pháp luật liên quan;

c) Chỉ đạo, 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, cụ thể như sau:

- Định kỳ 02 năm thực hiện kiểm tra, đánh giá an toàn thông tin[10] và quản lý rủi ro an toàn thông tin tổng thể trong hoạt động của cơ quan, tổ chức mình;

- Định kỳ hàng năm thực hiện kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin đối với các hệ thống cấp độ 3 và cấp độ 4;

- Định kỳ 06 tháng (hoặc đột xuất khi thấy cần thiết hoặc theo yêu cầu, cảnh báo của cơ quan chức năng) thực hiện kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin đối với hệ thống cấp độ 5;

- Việc kiểm tra, đánh giá an toàn thông tin và đánh giá rủi ro an toàn thông tin đối với hệ thống từ cấp độ 3 trở lên phải do tổ chức chuyên môn được cơ quan có thẩm quyền cấp phép; tổ chức sự nghiệp nhà nước có chức năng, nhiệm vụ phù hợp hoặc do tổ chức chuyên môn được cấp có thẩm quyền chỉ định thực hiện.

d) Chỉ đạo, tổ chức thực hiện đào tạo ngắn hạn, tuyên truyền, phổ biến, nâng cao nhận thức và diễn tập về an toàn thông tin, cụ thể như sau:

- Đào tạo, bồi dưỡng theo các chương trình đào tạo ngắn hạn nâng cao kiến thức, kỹ năng về an toàn thông tin cho cán bộ, công chức, viên chức làm về an toàn thông tin trong cơ quan, tổ chức mình;

- Tuyên truyền, phổ biến nâng cao nhận thức về an toàn thông tin cho cán bộ, công chức, viên chức trong cơ quan, tổ chức mình;

---

[9] Quy định này chi tiết hóa các quy định tại Điều 25. Trách nhiệm của chủ quản hệ thống thông tin của Luật An toàn thông tin mạng.

[10] Chi tiết các nội dung quy định về kiểm tra, đánh giá an toàn thông tin xem tại Điều 11 và Điều 12 Thông tư số 12/2022/TT-BTTTT.

- Diễn tập bảo đảm an toàn thông tin trong hoạt động của cơ quan, tổ chức mình; tham gia diễn tập quốc gia và diễn tập quốc tế do Bộ Thông tin và Truyền thông tổ chức.

đ) Chỉ đạo đơn vị vận hành hệ thống thông tin phối hợp với đơn vị chức năng liên quan của Bộ Thông tin và Truyền thông (Cục An toàn thông tin) trong việc triển khai thiết bị, kết nối tới hệ thống kỹ thuật xử lý, giảm thiểu tấn công mạng, hỗ trợ giám sát an toàn thông tin cho hệ thống thông tin cung cấp dịch vụ công trực tuyến, phát triển Chính phủ điện tử.

1.4. Xác định chủ quản hệ thống thông tin

Căn cứ quy định tại khoản 1 Điều 3 Nghị định số 85/2016/NĐ-CP và Điều 4 Thông tư số 12/2022/TT-BTTTT, chủ quản hệ thống thông tin xác định như sau:

1.4.1. 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

a) Mặc định: Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương (sau đây gọi chung là Ủy ban nhân dân cấp tỉnh) là chủ quản hệ thống thông tin của các hệ thống thông tin do các đơn vị (bao gồm đơn vị tham mưu, đơn vị hành chính, đơn vị sự nghiệp công lập và doanh nghiệp nhà nước) thuộc phạm vi quản lý làm chủ đầu tư.

b) Theo cấp có thẩm quyền quyết định đầu tư: Căn cứ quy định tại điểm c khoản 1 Điều 4 Thông tư số 12/2022/TT-BTTTT, đơn vị thuộc hoặc trực thuộc được bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân cấp tỉnh quyết định là chủ quản hệ thống thông tin đối với các hệ thống thông tin do đơn vị tự quyết định đầu tư, nếu đáp ứng hai điều kiện sau đây:

- Một là, có đủ năng lực thực thi quy định tại khoản 1 Điều 20 Nghị định số 85/2016/NĐ-CP, cụ thể:

+ Người đứng đầu đơn vị phải chỉ định được đơn vị trực thuộc làm đơn vị chuyên trách về an toàn thông tin theo quy định tại khoản 5 Điều 3 và điểm b khoản 1 Điều 20 Nghị định số 85/2016/NĐ-CP;

+ Đơn vị trực thuộc được chỉ định là đơn vị chuyên trách về an toàn thông tin phải đáp ứng các điều kiện được nêu tại **Mục 2.3.2 Chương 2**;

- Hai là, có đủ năng lực để thực thi đầy đủ các quy định tại khoản 2 Điều 20 Nghị định số 85/2016/NĐ-CP.

Lưu ý quan trọng: Việc xác định chủ quản hệ thống thông tin đối với các hệ thống thông tin tại các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân cấp tỉnh chỉ dựa trên cơ sở là bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân hoặc là cấp có thẩm quyền quyết định đầu tư, ***không xác định theo phân cấp hành chính***, do đó:

(1) Trường hợp theo phân cấp đầu tư, một đơn vị thuộc phạm vi quản lý của bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ hoặc Ủy ban nhân dân cấp

tỉnh là cấp có thẩm quyền quyết định đầu tư xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin *nhưng không đủ năng lực* làm chủ quản hệ thống thông tin hoặc *có đủ năng lực nhưng không được* bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ hoặc Ủy ban nhân dân cấp tỉnh quyết định là chủ quản hệ thống thông tin thì chủ quản hệ thống thông tin được xác định là bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ hoặc Ủy ban nhân dân cấp tỉnh tương ứng;

(2) Trường hợp cần phân cấp chủ quản hệ thống thông tin, bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân cấp tỉnh cần chỉ đạo đơn vị chuyên trách về an toàn thông tin có đánh giá cụ thể về năng lực của từng tổ chức để xác định những tổ chức có đủ năng lực làm chủ quản hệ thống thông tin, đặc biệt là đối với hệ thống thông tin được đề xuất cấp độ 4 và cấp độ 5.

Ví dụ 2.1. Một số trường hợp điển hình:

(i) Đối với các hệ thống thông tin (nếu có) do Ủy ban nhân dân cấp xã, Ủy ban nhân dân cấp huyện, Chi cục/Trung tâm thuộc Sở, cơ sở y tế công lập thuộc Sở Y tế, cơ sở giáo dục công lập thuộc Sở Giáo dục và Đào tạo, Sở, ban, ngành, doanh nghiệp nhà nước… tại địa phương quyết định đầu tư nhưng đơn vị không đủ năng lực làm chủ quản hệ thống thông tin thì chủ quản hệ thống thông tin được xác định là Ủy ban nhân dân cấp tỉnh;

(ii) Đối với các hệ thống thông tin (nếu có) do Văn phòng, Thanh tra, Cục, Chi cục/Trung tâm thuộc Cục, Chi cục thuộc Cục tại địa phương thuộc Tổng cục, Cục tại địa phương thuộc Tổng cục, Tổng cục, Ban, Trung tâm, Viện, Học viện, doanh nghiệp nhà nước… thuộc bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ quyết định đầu tư nhưng đơn vị không đủ năng lực làm chủ quản hệ thống thông tin thì chủ quản hệ thống thông tin được xác định là bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;

(iii) Trường hợp Tổng cục (và tương đương) thuộc bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ có đủ năng lực làm chủ quản nhưng theo phân cấp đầu tư, hệ thống thông tin do Cục/Trung tâm tại trung ương thuộc Tổng cục, Cục/Chi cục thuộc Cục tại địa phương thuộc Tổng cục… quyết định đầu tư và Cục, Chi cục thuộc Cục không đủ năng lực làm chủ quản hệ thống thông tin thì chủ quản hệ thống thông tin được xác định là bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ. Trường hợp bộ ủy quyền Tổng cục làm chủ quản hệ thống thông tin thì thực hiện theo quy định tại khoản 3 Điều 4 Thông tư số 12/2022/TT-BTTTT và hướng dẫn chi tiết tại **Mục 1.5 Chương 2** bên dưới.

1.4.2. Đối với doanh nghiệp và các tổ chức khác (không phải bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân cấp tỉnh, như cơ quan Đảng, Đoàn thể, Quốc hội, Hội đồng nhân dân các cấp; tổ chức chính trị, chính trị-xã hội…)

Chủ quản hệ thống thông tin được xác định là cấp có thẩm quyền quyết định đầu tư xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin.

Trường hợp một đơn vị là cấp có thẩm quyền quyết định đầu tư xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin *nhưng không đủ năng lực* làm chủ quản hệ thống thông tin, đơn vị đó cần báo cáo cơ quan, tổ chức cấp trên trực tiếp và đề nghị cơ quan, tổ chức cấp trên trực tiếp làm chủ quản hệ thống thông tin.

Ví dụ 2.2. Đối với hệ thống thông tin (nếu có) do các cơ quan Đảng xây dựng, triển khai, việc tổ chức bảo đảm an toàn hệ thống thông tin theo cấp độ được thực hiện theo Luật An toàn thông tin mạng và các văn bản quy định, hướng dẫn của Đảng, trong đó có thể tham khảo phương án thực hiện như sau:

(i) Đối với hệ thống thông tin (nếu có) do các cơ quan Đảng bộ cấp huyện, Đảng bộ khối, Văn phòng tỉnh ủy và các ban của Đảng tại địa phương quyết định đầu tư, tuy nhiên các đơn vị này không đủ năng lực làm chủ quản hệ thống thông tin thì khi đó, chủ quản hệ thống thông tin được xác định là Đảng bộ cấp tỉnh. Ban Thường vụ Đảng bộ tỉnh hoặc Ban chấp hành Đảng bộ tỉnh (theo thẩm quyền) cần chỉ định một đơn vị trực thuộc làm nhiệm vụ đơn vị chuyên trách về an toàn thông tin của Đảng bộ tỉnh theo quy định (thường là Văn phòng tỉnh ủy);

(ii) Đối với hệ thống thông tin (nếu có) do các đơn vị thuộc các Ban của Đảng ở trung ương quyết định đầu tư, tuy nhiên các đơn vị này không đủ năng lực làm chủ quản thì khi đó, chủ quản hệ thống thông tin được xác định là cơ quan Ban của Đảng ở trung ương. Lãnh đạo Ban của Đảng ở trung ương cần chỉ định một đơn vị trực thuộc làm nhiệm vụ đơn vị chuyên trách về an toàn thông tin theo quy định (thường là Văn phòng hoặc Trung tâm Thông tin trực thuộc).

Lưu ý: Đối với hệ thống thông tin (nếu có) do các đơn vị thuộc Văn phòng Quốc hội/Hội đồng nhân dân, Tòa án nhân dân, Viện Kiểm sát nhân dân, Kiểm toán nhà nước, Hội, Hiệp hội, Đoàn thể… ở trung ương hoặc địa phương quyết định đầu tư có thể tham khảo phương án thực hiện tại Ví dụ 2.2 ở trên để tổ chức triển khai.

1.5. Ủy quyền trách nhiệm chủ quản hệ thống thông tin

Trường hợp áp dụng khoản 3 Điều 4 Thông tư số 12/2022/TT-BTTTT, bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân cấp tỉnh có văn bản ủy quyền cho một đơn vị trực thuộc có đủ năng lực để thay mặt thực hiện trách nhiệm của chủ quản hệ thống thông tin theo quy định tại khoản 2 Điều 20 Nghị định 85/2016/NĐ-CP thì khi đó, theo quy định của pháp luật về dân sự:

(1) Đơn vị được ủy quyền không phải chủ quản hệ thống thông tin mà chỉ thực hiện các nhiệm vụ được chủ quản hệ thống thông tin ủy quyền (theo phạm vi nhiệm vụ được nêu trong văn bản ủy quyền);

(2) Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân cấp tỉnh vẫn là chủ quản hệ thống thông tin và đơn vị chuyên trách về an toàn thông tin của bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân cấp

tỉnh vẫn thực hiện trách nhiệm của mình đối với hệ thống thông tin (xem chi tiết tại **Mục 2.2 Chương 2** bên dưới);

(3) Trường hợp có hệ thống thông tin được đề xuất cấp độ 3 trở lên thì khi phê duyệt cấp độ an toàn thông tin (cấp độ 3, 4) hoặc phê duyệt phương án bảo đảm an toàn thông tin (cấp độ 5), Người đứng đầu đơn vị được ủy quyền ký quyết định của đơn vị ủy quyền (chủ quản hệ thống thông tin) với tư cách *thừa ủy quyền.*

2. Đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin

2.1. Định nghĩa

Đơn vị chuyên trách về an toàn thông tin[11] là đơn vị có chức năng, nhiệm vụ bảo đảm an toàn thông tin của chủ quản hệ thống thông tin.

2.2. Trách nhiệm của đơn vị chuyên trách về an toàn thông tin

Theo quy định tại Điều 21 Nghị định số 85/2016/NĐ-CP, đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin có trách nhiệm:

- Tham mưu, tổ chức thực thi, đôn đốc, kiểm tra, giám sát công tác bảo đảm an toàn thông tin;

- Thẩm định hồ sơ đề xuất cấp độ 1, 2, 3, phê duyệt cấp độ an toàn thông tin đối với các hệ thống thông tin được đề xuất cấp độ 1, 2 hoặc cho ý kiến về mặt chuyên môn đối với hồ sơ đề xuất cấp độ 4, 5 theo thẩm quyền quy định tại khoản 1, khoản 2 Điều 12 và Khoản 5 Điều 15 Nghị định số 85/2016/NĐ-CP.

Đơn vị chuyên trách về an toàn thông tin của các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ và Ủy ban nhân dân cấp tỉnh còn đảm nhận vai trò là đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng theo quy định tại Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia.

2.3. Chỉ định, thành lập đơn vị chuyên trách về an toàn thông tin

2.3.1. Trường hợp các cơ quan, tổ chức được xác định là chủ quản hệ thống thông tin, chưa có đơn vị chuyên trách về an toàn thông tin độc lập nhưng đã có đơn vị chuyên trách về công nghệ thông tin

Theo quy định tại điểm b khoản 1 Điều 20 Nghị định số 85/2016/NĐ-CP, Người đứng đầu cơ quan, tổ chức là chủ quản hệ thống thông tin có trách nhiệm:

- Chỉ định đơn vị chuyên trách về công nghệ thông tin làm nhiệm vụ đơn vị chuyên trách về an toàn thông tin;

- Thành lập hoặc chỉ định bộ phận chuyên trách về an toàn thông tin trực thuộc đơn vị chuyên trách về công nghệ thông tin.

[11] Theo khoản 5 Điều 3 Nghị định số 85/2016/NĐ-CP.

Bộ phận chuyên trách về an toàn thông tin[12] là bộ phận do chủ quản hệ thống thông tin thành lập hoặc chỉ định (thuộc đơn vị chuyên trách về công nghệ thông tin) để (tham mưu giúp đơn vị chuyên trách về công nghệ thông tin) thực thi nhiệm vụ bảo đảm an toàn thông tin và ứng cứu sự cố an toàn thông tin mạng (nhiệm vụ của đơn vị chuyên trách về an toàn thông tin).

2.3.2. Điều kiện xác định đơn vị chuyên trách về an toàn thông tin

Đơn vị được xác định là đơn vị chuyên trách về an toàn thông tin phải đáp ứng các điều kiện sau đây:

(1) Là một đơn vị trực thuộc của chủ quản hệ thống thông tin, có chức năng, nhiệm vụ bảo đảm an toàn thông tin hoặc được giao nhiệm vụ là đơn vị chuyên trách về công nghệ thông tin của chủ quản hệ thống thông tin;

(2) Có năng lực để bảo đảm thực thi các quy định tại Điều 21 Nghị định số 85/2016/NĐ-CP, trong đó: có nhân sự đáp ứng yêu cầu chuyên môn, đảm bảo tổ chức thẩm định hồ sơ đề xuất cấp độ; có tư cách pháp nhân để ban hành quyết định phê duyệt cấp độ an toàn thông tin đối với các hệ thống thông tin được đề xuất cấp độ 1, 2 theo thẩm quyền được giao tại khoản 1 Điều 12 Nghị định số 85/2016/NĐ-CP, phù hợp các quy định của pháp luật về dân sự và các quy định của pháp luật có liên quan.

Ví dụ 2.3. Đơn vị chuyên trách về an toàn thông tin tại các địa phương:

(i) Đối với Ủy ban nhân dân cấp tỉnh: Sở Thông tin và Truyền thông được xác định là đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin là Ủy ban nhân dân cấp tỉnh theo quy định tại điểm a khoản 15 Điều 2 Thông tư số 11/2022/TT-BTTTT ngày 29/7/2022 của Bộ trưởng Bộ Thông tin và Truyền thông hướng dẫn chức năng, nhiệm vụ, quyền hạn của Sở Thông tin và Truyền thông thuộc Ủy ban nhân dân cấp tỉnh, Phòng Văn hóa và Thông tin thuộc Ủy ban nhân dân cấp huyện;

(ii) Đối với Ủy ban nhân dân cấp huyện: Phòng Văn hóa và Thông tin thuộc Ủy ban nhân dân cấp huyện có thể được xem xét làm đơn vị chuyên trách về an toàn thông tin của Ủy ban nhân dân cấp huyện nếu đáp ứng các điều kiện nêu trên. Trường hợp Phòng Văn hóa và Thông tin đáp ứng điều kiện làm đơn vị chuyên trách về an toàn thông tin thì Ủy ban nhân dân cấp tỉnh xem xét năng lực làm chủ quản hệ thống thông tin của Ủy ban nhân dân cấp huyện trước khi quyết định phân cấp;

(iii) Đối với Ủy ban nhân dân cấp xã: Ủy ban nhân dân cấp xã không có đơn vị trực thuộc nên không có đơn vị chuyên trách về an toàn thông tin.

[12] Theo khoản 6 Điều 3 Nghị định số 85/2016/NĐ-CP.

3. Đơn vị vận hành hệ thống thông tin

3.1. Định nghĩa

Đơn vị vận hành hệ thống thông tin[13] là cơ quan, tổ chức được chủ quản hệ thống thông tin giao nhiệm vụ vận hành hệ thống thông tin.

3.2. Trách nhiệm của đơn vị vận hành hệ thống thông tin

Theo quy định tại Điều 22 Nghị định số 85/2016/NĐ-CP, đơn vị vận hành hệ thống thông tin có trách nhiệm:

- Thực hiện xác định cấp độ an toàn hệ thống thông tin theo quy định tại Điều 14 Nghị định số 85/2016/NĐ-CP;

- Thực hiện bảo vệ hệ thống thông tin theo quy định của pháp luật và hướng dẫn, tiêu chuẩn, quy chuẩn an toàn thông tin;

- Định kỳ đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin, báo cáo chủ quản hệ thống thông tin điều chỉnh nếu cần thiết;

- Định kỳ hoặc đột xuất báo cáo công tác thực thi bảo đảm an toàn hệ thống thông tin theo yêu cầu của chủ quản hệ thống thông tin hoặc cơ quan quản lý nhà nước chuyên ngành có thẩm quyền;

- Phối hợp, thực hiện theo yêu cầu của cơ quan chức năng liên quan của Bộ Thông tin và Truyền thông trong công tác bảo đảm an toàn thông tin.

3.3. 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

Theo quy định tại khoản 2 Điều 5 Thông tư số 12/2022/TT-BTTT, 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. Khi đó quy chế bảo đảm an toàn thông tin cần làm rõ trách nhiệm của đơn vị chủ trì và các đơn vị tham gia vận hành hệ thống thông tin.

4. Trách nhiệm của chủ đầu tư dự án, hoạt động ứng dụng công nghệ thông tin phục vụ xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin

4.1. Trong các giai đoạn chuẩn bị đầu tư, thực hiện đầu tư xây dựng dự án, hoạt động ứng dụng công nghệ thông tin

Mặc định chủ đầu tư được xác định là đơn vị vận hành hệ thống thông tin, chịu trách nhiệm:

(1) Lồng ghép thuyết minh đề xuất cấp độ vào nội dung báo cáo kinh tế - kỹ thuật (trường hợp dự án đầu tư áp dụng phương án thiết kế 01 bước), 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) hoặc đề cương và dự toán chi tiết (trong trường hợp đầu tư ứng dụng công nghệ thông tin không phải lập dự án)[14];

[13] Theo khoản 3 Điều 3 Nghị định số 85/2016/NĐ-CP.
[14] Khoản 1 Điều 13 Nghị định số 85/2016/NĐ-CP.

(2) Xây dựng hồ sơ đề xuất cấp độ an toàn hệ thống thông tin, đồng bộ với phương án kỹ thuật trong báo cáo kinh tế - kỹ thuật hoặc thiết kế cơ sở thuộc báo cáo nghiên cứu khả thi hoặc đề cương và dự toán chi tiết tương ứng[15];

(3) Khuyến khích gửi đơn vị/trình cấp có thẩm quyền thẩm định và phê duyệt cấp độ an toàn hệ thống thông tin 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 đề cương và dự toán chi tiết tương ứng[16].

Trường hợp chủ đầu tư đồng thời là cấp có thẩm quyền quyết định đầu tư, có đủ năng lực, được xác định là chủ quản hệ thống thông tin thì chủ đầu tư chỉ định một đơn vị hoặc bộ phận trực thuộc thực hiện nhiệm vụ đơn vị vận hành hệ thống thông tin. Khi đó, đơn vị hoặc bộ phận được xác định là đơn vị vận hành hệ thống thông tin sẽ chịu trách nhiệm thực hiện các nhiệm vụ (2) và (3) ở trên.

4.2. Trong giai đoạn vận hành cho đến khi kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin

Trên cơ sở từng tình huống cụ thể, chủ đầu tư có thể đóng vai trò:

(1) Chủ quản hệ thống thông tin nếu là cấp có thẩm quyền quyết định đầu tư dự án xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin đó và có đủ năng lực để thực thi đầy đủ các quy định tại Điều 20 Nghị định 85/2016/NĐ-CP, được quyết định là chủ quản hệ thống thông tin, hoặc;

(2) Tiếp tục là đơn vị vận hành hệ thống thông tin nếu chủ quản hệ thống thông tin không có văn bản giao một đơn vị khác thực hiện nhiệm vụ đơn vị vận hành hệ thống thông tin, hoặc;

(3) Đơn vị tham gia sử dụng hệ thống thông tin nếu chủ quản hệ thống thông tin có văn bản giao một đơn vị khác thực hiện nhiệm vụ đơn vị vận hành hệ thống thông tin. Khi đó quy chế bảo đảm an toàn thông tin cho hệ thống cần làm rõ trách nhiệm giữa đơn vị vận hành hệ thống thông tin và đơn vị tham gia sử dụng hệ thống thông tin.

Ví dụ 2.4. Trong giai đoạn vận hành hệ thống thông tin, chủ đầu tư cài đặt, vận hành hệ thống thông tin tại Trung tâm dữ liệu của bộ/địa phương do đơn vị chuyên trách về công nghệ thông tin của bộ/địa phương quản lý hoặc chủ đầu tư thuê dịch vụ hạ tầng số và cài đặt, vận hành hệ thống thông tin tại Trung tâm dữ liệu hoặc dịch vụ điện toán đám mây của doanh nghiệp. Khi đó:

(i) Chủ đầu tư tiếp tục thực hiện nhiệm vụ là đơn vị vận hành hệ thống thông tin nếu chủ quản hệ thống thông tin không có văn bản giao đơn vị chuyên trách về công nghệ thông tin hoặc doanh nghiệp cung cấp dịch vụ hạ tầng số thực hiện nhiệm vụ đơn vị vận hành hệ thống thông tin;

(ii) Quy chế bảo đảm an toàn thông tin cho hệ thống cần làm rõ trách nhiệm giữa đơn vị vận hành hệ thống thông tin và đơn vị cung cấp dịch vụ hạ

[15] Khoản 1 Điều 8 Thông tư số 12/2022/TT-BTTTT.
[16] Điều 15 Thông tư số 12/2022/TT-BTTTT.

tầng số phục vụ vận hành hệ thống thông tin (hai đơn vị có thể ký quy chế phối hợp hoặc đồng trình chủ quản hệ thống thông tin ban hành).

5. Xác định các chủ thể khi thuê dịch vụ công nghệ thông tin không có sẵn trên thị trường

Khái niệm: *Dịch vụ công nghệ thông tin không sẵn có trên thị trường*[17] là dịch vụ được thiết lập theo các yêu cầu riêng nhằm đáp ứng yêu cầu đặc thù của cơ quan, đơn vị.

Đặc điểm:

(1) Cơ quan, đơn vị thuê tổ chức, cá nhân thiết lập mới, mở rộng hoặc nâng cấp cho hệ thống hạ tầng kỹ thuật, phần mềm, cơ sở dữ liệu nhằm đáp ứng yêu cầu đặc thù của cơ quan, đơn vị;

(2) Có hình thành hệ thống thông tin riêng của cơ quan, đơn vị thuê;

(3) Sau khi hoàn thành hệ thống hoặc hạng mục của hệ thống công nghệ thông tin thì tổ chức, cá nhân được thuê sẽ tổ chức quản trị, vận hành để cung cấp dịch vụ cho cơ quan, đơn vị thuê hoặc bàn giao cho cơ quan, đơn vị thuê tự tổ chức quản trị, vận hành trong một thời hạn nhất định.

Tổ chức thực hiện: Trường hợp bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ hoặc Ủy ban nhân dân cấp tỉnh hoặc đơn vị trực thuộc lựa chọn hình thức thuê dịch vụ công nghệ thông tin để xây dựng mới hoặc mở rộng, nâng cấp hệ thống thông tin theo yêu cầu đặc thù của cơ quan, đơn vị thì việc xác định các chủ thể có liên quan của hệ thống thông tin được xác định như trường hợp lập dự án hoặc xây dựng đề cương và dự toán chi tiết, cụ thể:

(1) Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân cấp tỉnh hoặc cấp có thẩm quyền quyết định đầu tư là chủ quản hệ thống thông tin.

(2) Khi chưa xác định được đơn vị cung cấp dịch vụ theo quy định pháp luật:

- Trường hợp chủ quản hệ thống thông tin thuê ngoài dịch vụ công nghệ thông tin (đồng thời là đơn vị chủ trì, trực tiếp ký hợp đồng thuê dịch vụ công nghệ thông tin): Chủ quản hệ thống thông tin giao một đơn vị trực thuộc tham mưu thực hiện (1) lồng ghép thuyết minh đề xuất cấp độ vào nội dung kế hoạch thuê dịch vụ[18]; (2) xây dựng hồ sơ đề xuất cấp độ an toàn hệ thống thông tin, đồng bộ với phương án kỹ thuật trong kế hoạch thuê dịch vụ[19]; (3) khuyến khích gửi đơn vị/trình cấp có thẩm quyền thẩm định và phê duyệt cấp độ an toàn hệ thống thông tin trước khi cấp có thẩm quyền phê duyệt kế hoạch thuê dịch vụ[20];

- Trường hợp chủ quản hệ thống thông tin giao một đơn vị trực thuộc chủ trì thuê dịch vụ công nghệ thông tin: Đơn vị chủ trì thuê dịch vụ được xác định là đơn vị vận hành hệ thống thông tin, tiến hành (1) lồng ghép thuyết minh đề

[17] Khoản 4 Điều 3 Nghị định số 73/2019/NĐ-CP ngày 05/9/2019 của Chính phủ quy định quản lý đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước.
[18] Khoản 2 Điều 13 Nghị định số 85/2016/NĐ-CP.
[19] Khoản 1 Điều 8 Thông tư số 12/2022/TT-BTTTT.
[20] Điều 15 Thông tư số 12/2022/TT-BTTTT.

xuất cấp độ vào nội dung kế hoạch thuê dịch vụ[21]; (2) xây dựng hồ sơ đề xuất cấp độ an toàn hệ thống thông tin, đồng bộ với phương án kỹ thuật trong kế hoạch thuê dịch vụ[22]; (3) khuyến khích gửi đơn vị/trình cấp có thẩm quyền thẩm định và phê duyệt cấp độ an toàn hệ thống thông tin trước khi cấp có thẩm quyền phê duyệt kế hoạch thuê dịch vụ[23].

(3) Khi đã xác định được đơn vị cung cấp dịch vụ theo quy định pháp luật:

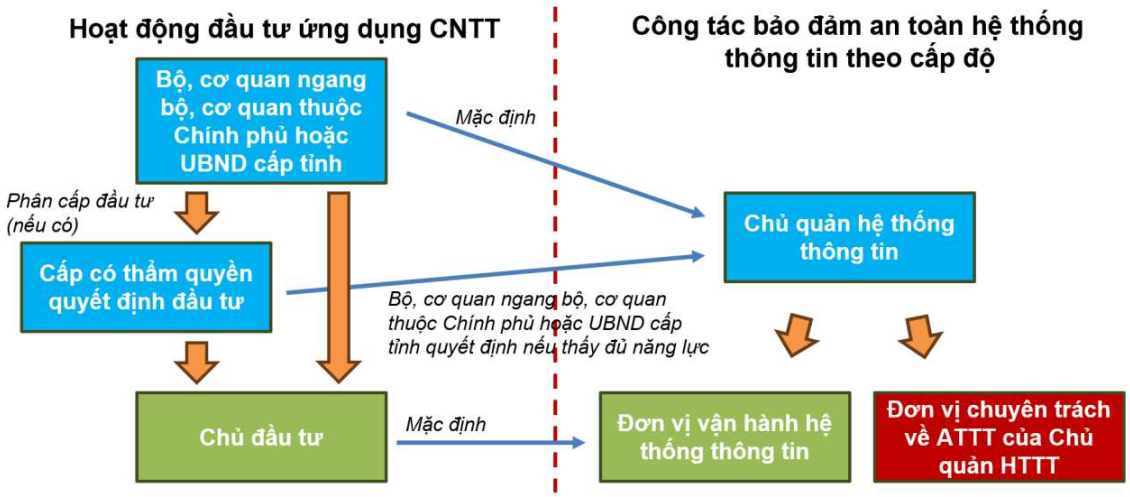
- Trường hợp chủ quản hệ thống thông tin thuê ngoài dịch vụ công nghệ thông tin (đồng thời là đơn vị chủ trì, trực tiếp ký hợp đồng thuê dịch vụ công nghệ thông tin): Theo quy định tại khoản 3 Điều 3 Nghị định số 85/2016/NĐ-CP, đơn vị vận hành là đơn vị cung cấp dịch vụ;

- Trường hợp chủ quản hệ thống thông tin giao một đơn vị trực thuộc chủ trì thuê dịch vụ công nghệ thông tin: Đơn vị chủ trì thuê dịch vụ tiếp tục là đơn vị vận hành nếu chủ quản hệ thống thông tin không giao đơn vị cung cấp dịch vụ hoặc đơn vị khác thực hiện nhiệm vụ đơn vị vận hành hệ thống thông tin.

Đơn vị cung cấp dịch vụ có trách nhiệm phối hợp với chủ quản hệ thống thông tin/đơn vị chủ trì thuê dịch vụ cập nhật thông tin trong hồ sơ đề xuất cấp độ theo đúng hiện trạng hạ tầng đã cài đặt để tổ chức thẩm định, phê duyệt (nếu chưa phê duyệt) hoặc gửi đơn vị chuyên trách về an toàn thông tin để cập nhật.

(4) Khi hết thời hạn cung cấp dịch vụ, nếu hệ thống thông tin tiếp tục được duy trì hoạt động (có thể chuyển về vận hành tại hạ tầng của đơn vị chủ trì thuê dịch vụ hoặc của chủ quản hệ thống thông tin…), thì đơn vị chủ trì thuê dịch vụ được xác định là đơn vị vận hành hệ thống thông tin.

TỔNG KẾT CHƯƠNG 2



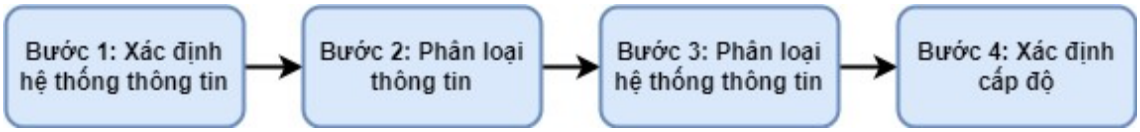
Hình 2. Xác định các chủ thể có liên quan

[21] Khoản 2 Điều 13 Nghị định số 85/2016/NĐ-CP.
[22] Khoản 1 Điều 8 Thông tư số 12/2022/TT-BTTTT.
[23] Điều 15 Thông tư số 12/2022/TT-BTTTT.

Chương 3.
Xác định cấp độ an toàn hệ thống thông tin

Cấp độ an toàn hệ thống thông tin được xác định dựa trên thông tin mà hệ thống thông tin đó xử lý và loại hình mà hệ thống thông tin đó được phân loại. Trên cơ sở đó, tiêu chí xác định cấp độ sẽ là tập các điều kiện giữa (1) loại thông tin hệ thống đó xử lý và (2) loại hình mà hệ thống thông tin được phân loại.

Chương này sẽ hướng dẫn chi tiết cách thức xác định cấp độ an toàn cho các hệ thống thông tin với 04 bước cơ bản.



Hình 3. Các bước xác định cấp độ an toàn thông tin cho hệ thống thông tin

1. Nguyên tắc xác định cấp độ

Nguyên tắc xác định cấp độ an toàn hệ thống thông tin được quy định tại Điều 5 Nghị định số 85/2016/NĐ-CP, cụ thể như sau:

(1) Việc xác định hệ thống thông tin để xác định cấp độ căn cứ trên nguyên tắc như sau:

- Mỗi hệ thống thông tin ***chỉ có một*** chủ quản hệ thống thông tin;

- Mỗi 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 thuộc một trong các loại hình hệ thống thông tin quy định tại khoản 2 Điều 6 Nghị định Nghị định số 85/2016/NĐ-CP.

(2) Trong trường hợp hệ thống thông tin bao gồm nhiều hệ thống thành phần, mỗi hệ thống thành phần lại tương ứng với một cấp độ khác nhau, thì cấp độ hệ thống thông tin được xác định ***là cấp độ cao nhất*** trong các cấp độ của các hệ thống thành phần cấu thành.

2. Bước 1. Xác định hệ thống thông tin

Trước hết cần làm rõ các thông tin sau đây:

(1) Tên hệ thống thông tin: Cần được thuyết minh thống nhất giữa các tài liệu báo cáo chủ trương đầu tư, báo cáo khảo sát, báo cáo kinh tế - kỹ thuật, báo cáo nghiên cứu khả thi dự án hoặc kế hoạch thuê dịch vụ công nghệ thông tin hoặc đề cương và dự toán chi tiết hoạt động ứng dụng công nghệ thông tin…;

(2) Các thành phần cấu thành hệ thống thông tin (phần cứng, phần mềm, cơ sở dữ liệu, mạng), đảm bảo hoạt ứng dụng công nghệ thông tin được đầu tư, thuê hoặc đang vận hành đáp ứng tiêu chí hình thành một hệ thống thông tin;

(3) Các chủ thể có liên quan: Chủ quản hệ thống thông tin, đơn vị chuyên trách về an toàn thông tin và đơn vị vận hành hệ thống thông tin.

3. Bước 2. Phân loại thông tin

Theo quy định tại Điều 9 Luật An toàn thông tin mạng, "Cơ quan, tổ chức sở hữu thông tin phân loại thông tin theo thuộc tính bí mật để có biện pháp bảo vệ phù hợp". Bên cạnh đó, "Thông tin thuộc phạm vi bí mật nhà nước được phân loại và bảo vệ theo quy định của pháp luật về bảo vệ bí mật nhà nước". Theo đó, căn cứ quy định tại khoản 1 Điều 6 Nghị định số 85/2016/NĐ-CP, thông tin được xử lý thông qua hệ thống thông tin được phân loại theo thuộc tính bí mật như sau:

a) *Thông tin công cộng* là thông tin trên mạng của một tổ chức, cá nhân được công khai cho tất cả các đối tượng mà không cần xác định danh tính, địa chỉ cụ thể của các đối tượng đó (không cần tài khoản, đăng nhập tài khoản để tiếp cận);

b) *Thông tin riêng* là thông tin trên mạng của một tổ chức, cá nhân mà tổ chức, cá nhân đó không công khai hoặc chỉ công khai cho một hoặc một nhóm đối tượng đã được xác định danh tính, địa chỉ cụ thể (cần tài khoản, đăng nhập tài khoản để tiếp cận0;

c) *Thông tin cá nhân* là thông tin trên mạng gắn với việc xác định danh tính một người cụ thể;

d) *Thông tin bí mật nhà nước* là thông tin ở mức Mật, Tối Mật, Tuyệt Mật theo quy định của pháp luật về bảo vệ bí mật nhà nước.

Các loại thông tin ở trên được phân loại theo *tính bí mật tăng dần* từ thông tin công cộng >> thông tin riêng, thông tin cá nhân >> thông tin bí mật nhà nước. Khi xác định cấp độ an toàn thông tin, căn cứ theo các loại thông tin mà hệ thống xử lý, ta chỉ cần xác định loại thông tin nào có tính bí mật cao nhất, loại thông tin đó sẽ quyết định cấp độ an toàn thông tin của hệ thống thông tin.

Ví dụ 3.1: Hệ thống thông tin có xử lý thông tin riêng hoặc thông tin cá nhân thì cấp độ an toàn thông tin tối thiểu là cấp độ 2; hệ thống thông tin có xử lý thông tin bí mật nhà nước thì cấp độ an toàn thông tin tối thiểu là cấp độ 3…

Khái niệm xử lý thông tin được quy định tại khoản 2 Điều 3 Nghị định số 85/2016/NĐ-CP như sau: *Xử lý thông tin* là việc thực hiện một hoặc một số thao tác tạo lập, cung cấp, thu thập, biên tập, sử dụng, lưu trữ, truyền đưa, chia sẻ, trao đổi thông tin trên mạng.

4. Bước 3. Phân loại hệ thống thông tin

Căn cứ quy định tại khoản 2 Điều 6 Nghị định số 85/2016/NĐ-CP, hệ thống thông tin được phân loại *theo chức năng phục vụ hoạt động nghiệp vụ*.

Bên cạnh đó, theo quy định tại khoản 7 Điều 7 Thông tư số 12/2022/TT-BTTTT, Cục An toàn thông tin 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 7 Thông tư, dưới đây là hướng dẫn đối với từng danh mục hệ thống thông tin, cụ thể như sau:

4.1. Hệ thống thông tin phục vụ hoạt động nội bộ

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, gồm các hệ thống thông tin điển hình như:

a) Trang, cổng thông tin điện tử nội bộ;

b) Hệ thống họp, hội nghị trực tuyến nội bộ;

c) Hệ thống thư điện tử nội bộ;

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

đ) Hệ thống đào tạo trực tuyến nội bộ;

e) Hệ thống thông tin phục vụ hoạt động nghiệp vụ trong phạm vi nội bộ của một hoặc có sự tham gia sử dụng trực tiếp của nhiều cơ quan, tổ chức nhưng không có sự tham gia sử dụng của người dân, doanh nghiệp (thuộc loại hình hệ thống thông tin phụ vụ người dân, doanh nghiệp).

4.2. Hệ thống thông tin phục vụ người dân, doanh nghiệp

Hệ thống thông tin phục vụ người dân, doanh nghiệp là hệ thống trực tiếp hoặc hỗ trợ cung cấp dịch vụ trực tuyến, gồm các hệ thống thông tin điển hình như:

a) Trang, cổng thông tin điện tử có cung cấp dịch vụ trực tuyến phục vụ người dân, doanh nghiệp;

b) Hệ thống họp, hội nghị trực tuyến phục vụ người dân, doanh nghiệp;

c) Hệ thống thư điện tử dùng phục vụ người dân và các doanh nghiệp;

d) Hệ thống quản lý văn bản và điều hành phục vụ các doanh nghiệp;

đ) Mạng xã hội;

e) Hệ thống tiếp nhận, giải quyết thủ tục hành chính, cung cấp dịch vụ công trực tuyến;

g) Hệ thống cung cấp dữ liệu mở;

h) Hệ thống phục vụ cơ chế một cửa quốc gia.

Lưu ý:

(1) Trong khái niệm về *hệ thống thông tin phục vụ người dân, doanh nghiệp* được nêu ở trên, *dịch vụ trực tuyến*[24] được hiểu là dịch vụ do doanh nghiệp hoặc cơ quan nhà nước cung cấp trên môi trường mạng cho các tổ chức, cá nhân.

Ví dụ 3.2. Một số dịch vụ trực tuyến điển hình phục vụ người dân, doanh nghiệp như: Dịch vụ báo chí, trò chơi điện tử, thương mại điện tử, thư điện tử…

(2) *Hệ thống hỗ trợ cung cấp dịch vụ trực tuyến* là các hệ thống thông tin được kết nối với hệ thống trực tiếp cung cấp dịch vụ trực tuyến nhằm hỗ trợ xử lý một hoặc một số hoạt động nghiệp vụ.

[24] Theo khoản 7 Điều 3 Nghị định số 85/2016/NĐ-CP.

Ví dụ 3.3. Hệ thống hỗ trợ cung cấp dịch vụ trực tuyến điển hình:

(i) Hệ thống một cửa điện tử cấp bộ, cấp tỉnh (có kết nối tiếp nhận hồ sơ từ Cổng dịch vụ công cấp bộ, cấp tỉnh - trực tiếp cung cấp dịch vụ trực tuyến phục vụ người dân, doanh nghiệp);

(ii) Các hệ thống thông tin nghiệp vụ do cơ quan trung ương hoặc địa phương triển khai có kết nối liên thông với Hệ thống một cửa điện tử cấp bộ, cấp tỉnh để hỗ trợ giải quyết thủ tục hành chính trực tuyến có thể được xem xét là hệ thống hỗ trợ cung cấp dịch vụ trực tuyến…

4.3. Hệ thống cơ sở hạ tầng thông tin

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), gồm các hệ thống thông tin điển hình như:

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

b) Trung tâm dữ liệu, điện toán đám mây;

c) Hệ thống giám sát điều hành thông minh (IOC);

d) Hệ thống giám sát điều hành an toàn thông tin mạng (SOC);

đ) Hệ thống định danh, xác thực điện tử, chứng thực điện tử, chữ ký số;

e) Hệ thống kết nối tích hợp, chia sẻ dữ liệu giữa các hệ thống thông tin;

g) Hệ thống giám sát, điều hành hoạt động của hệ thống thông tin điều khiển công nghiệp;

h) Hệ thống tổng hợp, phân tích dữ liệu;

i) Cơ sở dữ liệu tập trung;

k) Hệ thống lưu trữ, sao lưu dữ liệu tập trung;

l) Hệ thống thông tin phục vụ lưu trữ dữ liệu tập trung đối với một số loại hình thông tin, dữ liệu đặc biệt quan trọng của quốc gia là các hệ thống cơ sở dữ liệu quốc gia phục vụ ứng dụng công nghệ thông tin cho 11 lĩnh vực theo Quyết định số 632/QĐ-TTg ngày 10/5/2017 của Thủ tướng Chính phủ về việc ban hành Danh mục lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng và hệ thống thông tin quan trọng quốc gia.

4.4. Hệ thống thông tin điều khiển công nghiệp

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, gồm các hệ thống thông tin điển hình như:

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

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

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

d) Các hệ thống khác trực tiếp điều khiển, vận hành hoạt động bình thường của các công trình xây dựng.

4.5. Hệ thống thông tin khác

Hệ thống thông tin khác là các hệ thống thông tin không thuộc các hệ thống thông tin được mô tả tại các Mục 4.1, 4.2, 4.3, 4.4 ở trên và 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 hoặc được dùng chung giữa nhiều cơ quan, tổ chức theo lĩnh vực chuyên ngành.

5. Bước 4. Xác định cấp độ an toàn hệ thống thông tin

Các tiêu chí xác định cấp độ an toàn hệ thống thông tin từ cấp độ 1 đến cấp độ 5 tương ứng được quy định từ Điều 7 đến Điều 11 Nghị định số 85/2016/NĐ-CP, theo đó, để xác định đúng cấp độ an toàn thông tin, đơn vị vận hành hệ thống thông tin cần làm rõ quy mô và phạm vi triển khai của hệ thống thông tin, cụ thể:

5.1. Hệ thống thông tin cấp độ 1

Căn cứ quy định tại Điều 7 Nghị định số 85/2016/NĐ-CP:

Tiêu chí xác định: *Hệ thống thông tin phục vụ hoạt động nội bộ* của cơ quan, tổ chức và *chỉ xử lý thông tin công cộng*.

Ví dụ 3.4. Trang thông tin điện tử nội bộ, trang thông tin điện tử tổng hợp của cơ quan, đơn vị chỉ hoạt động theo quy định tại Điều 20 Nghị định số 72/2013/NĐ-CP ngày 15/7/2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng, không xử lý thông tin riêng, thông tin cá nhân, thông tin bí mật nhà nước và không cung cấp, hỗ trợ cung cấp các dịch vụ trực tuyến cho người dân, doanh nghiệp.

5.2. Hệ thống thông tin cấp độ 2

Căn cứ các quy định tại Điều 8 Nghị định số 85/2016/NĐ-CP, hệ thống thông tin cấp độ 2 là hệ thống thông tin đáp ứng một trong các tiêu chí cụ thể như sau:

(1) Tiêu chí 1: *Hệ thống thông tin phục vụ hoạt động nội bộ* của cơ quan, tổ chức và *có xử lý thông tin riêng, thông tin cá nhân* của người sử dụng nhưng *không xử lý thông tin bí mật nhà nước*.

Ví dụ 3.5. Một số trường hợp điển hình:

(i) Trang thông tin điện tử nội bộ, trang thông tin điện tử tổng hợp của cơ quan, đơn vị có xử lý thông tin riêng, thông tin cá nhân của người sử dụng (như phải có tài khoản đăng nhập để xem lịch công tác hoặc xem thông báo riêng…);

(ii) Hệ thống quản lý văn bản và điều hành; hệ thống quản lý cán bộ, công chức; hệ thống thư điện tử; hệ thống họp, hội nghị trực tuyến; hệ thống truyền

thanh thông minh ở trung ương hoặc tại địa phương… phục vụ hoạt động nội bộ của một cơ quan, đơn vị hoặc triển khai trên phạm vi một bộ, một tỉnh;

(iii) Hệ thống quản lý khám chữa bệnh tại các bệnh viện chưa tích hợp giải pháp cung cấp hoặc hỗ trợ cung cấp dịch vụ đăng ký khám chữa bệnh trực tuyến, *không lưu trữ hồ sơ bệnh án, thông tin, kết quả khám bệnh, chữa bệnh, kiểm tra sức khỏe của các đồng chí Ủy viên Bộ Chính trị, Ban Bí thư Trung ương Đảng*;

(iv) Hệ thống thông tin xử lý nghiệp vụ dùng chung triển khai cho các đơn vị xử lý nghiệp vụ của một ngành/lĩnh vực trên toàn quốc, không cung cấp, hỗ trợ cung cấp dịch vụ trực tuyến cho người dân, doanh nghiệp…

(2) Tiêu chí 2: *Hệ thống thông tin phục vụ người dân, doanh nghiệp* thuộc một trong các loại hình như sau:

- Cung cấp thông tin và dịch vụ công trực tuyến từ mức độ 2 trở xuống theo quy định của pháp luật (cung cấp dịch vụ công trực tuyến một phần theo quy định tại Nghị định số 42/2022/NĐ-CP ngày 24/6/2022 của Chính phủ quy định về việc cung cấp thông tin và dịch vụ công trực tuyến của cơ quan nhà nước trên môi trường mạng, thay thế Nghị định số 43/2011/NĐ-CP, trong đó không hỗ trợ chức năng cho phép người sử dụng điền và gửi trực tuyến các mẫu văn bản đến cơ quan, tổ chức cung cấp dịch vụ hoặc có hỗ trợ nhưng các giao dịch trong quá trình xử lý hồ sơ và cung cấp dịch vụ không được thực hiện trên môi trường mạng);

- Cung cấp dịch vụ trực tuyến không thuộc danh mục dịch vụ kinh doanh có điều kiện (theo quy định của Luật Đầu tư năm 2020);

- Cung cấp dịch vụ trực tuyến khác có xử lý thông tin riêng, thông tin cá nhân của dưới 10.000 người sử dụng (số lượng người sử dụng được tính theo số tài khoản người dùng tương ứng tham gia sử dụng hệ thống thông tin).

Ví dụ 3.6. Một số trường hợp điển hình:

(i) Trang thông tin điện tử của cơ quan, tổ chức có cung cấp dịch vụ trực tuyến cho người dân, doanh nghiệp đáp ứng tối thiểu một trong các tiêu chí ở trên và chưa đạt một trong các tiêu chí hệ thống thông tin cấp độ 3 theo quy định tại khoản 2 Điều 9 Nghị định số 85/2016/NĐ-CP (xem chi tiết tại Tiêu chí 2 **Mục 5.3 Chương 3** bên dưới);

(ii) Báo điện tử, tạp chí điện tử hoạt động theo quy định của Luật Báo chí, không có tương tác xử lý thông tin cá nhân của người sử dụng hoặc có tương tác xử lý thông tin cá nhân của dưới 10.000 người sử dụng dịch vụ;

(iii) Nền tảng số eOffice, nền tảng số thư điện tử, nền tảng số họp, hội nghị trực tuyến… triển khai cho người dân, doanh nghiệp có dưới 10.000 người sử dụng;

(iv) Nền tảng học trực tuyến, nên tảng lưu trữ tài liệu trực tuyến mới triển khai cho dưới 10.000 người sử dụng;

(v) Hệ thống quản lý khám chữa bệnh tại các bệnh viện đã tích hợp giải pháp cung cấp hoặc hỗ trợ cung cấp các dịch vụ đăng ký khám chữa bệnh trực tuyến, trong đó số bệnh nhân đã tham gia đăng ký khám chữa bệnh trực tuyến mới ở mức dưới 10.000 người và *không lưu trữ hồ sơ bệnh án, thông tin, kết quả khám bệnh, chữa bệnh, kiểm tra sức khỏe của các đồng chí Ủy viên Bộ Chính trị, Ban Bí thư Trung ương Đảng …*

(3) Tiêu chí 3: *Hệ thống cơ sở hạ tầng thông tin* phục vụ hoạt động của một cơ quan, tổ chức.

Ví dụ 3.7. Một số trường hợp điển hình như Trung tâm dữ liệu, Mạng viễn thông dùng riêng theo quy định của Luật Viễn thông (như Hệ thống tổng đài điện thoại nộ bộ), cơ sở dữ liệu nội bộ, Hệ thống tổng hợp, phân tích dữ liệu nội bộ… của một cơ quan, tổ chức.

5.3. Hệ thống thông tin cấp độ 3

Căn cứ Điều 9 Nghị định số 85/2016/NĐ-CP, hệ thống thông tin cấp độ 3 là hệ thống thông tin có một trong các tiêu chí cụ thể như sau:

(1) Tiêu chí 1: Hệ thống thông tin *xử lý thông tin bí mật nhà nước* hoặc hệ thống phục vụ quốc phòng, an ninh khi bị phá hoại sẽ làm *tổn hại tới quốc phòng, an ninh quốc gia*.

Lưu ý: Việc xác định hệ thống thông tin có xử lý thông tin bí mật nhà nước có thể dựa trên cơ sở các Quyết định của Thủ tướng ban hành danh mục bí mật nhà nước trong từng lĩnh vực cụ thể.

Ví dụ 3.8. Một số trường hợp điển hình:

(i) Quyết định số 960/QĐ-TTg ngày 07/7/2020 của Thủ tướng Chính phủ ban hành danh mục bí mật nhà nước lĩnh vực nội vụ có quy định "hồ sơ nhân sự đối với chức danh cán bộ, công chức, viên chức và các chức danh lãnh đạo, quản lý thuộc thẩm quyền của Thủ tướng Chính phủ quyết định phê chuẩn chưa công khai" là bí mật nhà nước mức độ Mật. Do đó, trường hợp Hệ thống quản lý cán bộ tại các bộ, ngành, địa phương có lưu trữ thông tin trên thì phải xác định là hệ thống thông tin là cấp độ 3 (hoặc cấp độ 4, cấp độ 5 tùy thuộc vào đánh giá về mức độ tổn hại khi bị phá hoại);

(ii) Quyết định số 1295/QĐ-TTg ngày 24/8/2020 của Thủ tướng Chính phủ ban hành danh mục bí mật nhà nước lĩnh vực y tế có quy định "Hồ sơ bệnh án, thông tin, kết quả khám bệnh, chữa bệnh, kiểm tra sức khỏe của các đồng chí Ủy viên Bộ Chính trị, Ban Bí thư Trung ương Đảng" là bí mật nhà nước mức độ Tối Mật và "Số người mắc, người chết do bệnh truyền nhiễm nguy hiểm mới phát sinh chưa rõ tác nhân gây bệnh chưa được Bộ Y tế công khai" là bí mật nhà nước mức độ Mật. Do đó, trường hợp Hệ thống quản lý khám chữa bệnh tại các bệnh viện có lưu trữ các thông tin trên thì phải xác định là hệ thống thông tin là cấp độ 3 (hoặc cấp độ 4, cấp độ 5 tùy thuộc vào đánh giá về mức độ tổn hại khi bị phá hoại).

(2) Tiêu chí 2: *Hệ thống thông tin phục vụ người dân, doanh nghiệp* thuộc một trong các loại hình như sau:

- Cung cấp thông tin và dịch vụ công trực tuyến từ mức độ 3 trở lên theo quy định của pháp luật (cung cấp dịch vụ công trực tuyến toàn trình hoặc một phần theo quy định tại Nghị định số 42/2022/NĐ-CP, trong đó, hỗ trợ chức năng cho phép người sử dụng điền và gửi trực tuyến các mẫu văn bản đến cơ quan, tổ chức cung cấp dịch vụ, đồng thời, các giao dịch trong quá trình xử lý hồ sơ và cung cấp dịch vụ được thực hiện trên môi trường mạng);

- Cung cấp dịch vụ trực tuyến thuộc danh mục dịch vụ kinh doanh có điều kiện (theo quy định của Luật Đầu tư năm 2020);

- Cung cấp dịch vụ trực tuyến khác có xử lý thông tin riêng, thông tin cá nhân của từ 10.000 người sử dụng trở lên.

Ví dụ 3.9. Một số trường hợp điển hình:

(i) Cổng dịch vụ công, hệ thống một cửa điện tử cấp bộ, cấp tỉnh;

(ii) Cổng thông tin điện tử theo quy định tại Nghị định số 42/2022/NĐ-CP và Thông tư số 22/2023/TT-BTTTT ngày 31/12/2023 của Bộ trưởng Bộ Thông tin và Truyền thông quy định cấu trúc, bố cục, yêu cầu kỹ thuật cho cổng thông tin điện tử và trang thông tin điện tử của cơ quan nhà nước;

(iii) Hệ thống thương mại điện tử, hệ thống cung cấp dịch vụ bưu chính (dịch vụ kinh doanh có điều kiện);

(iv) Báo điện tử, tạp chí điện tử theo quy định của Luật Báo chí có tương tác xử lý thông tin từ 10.000 người sử dụng dịch vụ trở lên;

(v) Nền tảng học trực tuyến, nền tảng lưu trữ tài liệu trực tuyến đã triển khai từ 10.000 người sử dụng trở lên;

(vi) Nền tảng số eOffice, nền tảng số thư điện tử, nền tảng số họp, hội nghị trực tuyến… triển khai cho các cơ quan, doanh nghiệp trong đó phạm vi triển khai từ 10.000 người sử dụng trở lên;

(vii) Hệ thống quản lý khám chữa bệnh tại các bệnh viện đã tích hợp giải pháp cung cấp hoặc hỗ trợ cung cấp các dịch vụ đăng ký khám chữa bệnh trực tuyến trong đó số bệnh nhân đã tham gia đăng ký khám chữa bệnh trực tuyến đã từ 10.000 người trở lên *(có lưu trữ hoặc không lưu trữ hồ sơ bệnh án, thông tin, kết quả khám bệnh, chữa bệnh, kiểm tra sức khỏe của các đồng chí Ủy viên Bộ Chính trị, Ban Bí thư Trung ương Đảng)*…

(3) Tiêu chí 3: *Hệ thống cơ sở hạ tầng thông tin dùng chung* phục vụ hoạt động của các cơ quan, tổ chức trong phạm vi một ngành, một tỉnh / một số tỉnh.

Ví dụ 3.10. Một số trường hợp điển hình như:

(i) Trung tâm dữ liệu, điện toán đám mây cấp bộ, cấp tỉnh;

(ii) Nền tảng tích hợp, chia sẻ dữ liệu cấp Bộ, cấp tỉnh; Mạng truy nhập cấp II tại các bộ, ngành, địa phương;

(iii) Cơ sở dữ liệu chuyên ngành hoặc dùng chung trong phạm vi một tỉnh hoặc một số tỉnh hoặc một ngành trong phạm vi toàn quốc nhưng không yêu cầu vận hành 24/7, chấp nhận ngừng vận hành mà không có kế hoạch trước;

(iv) Hệ thống giám sát điều hành thông minh (IOC), Hệ thống giám sát điều hành an toàn thông tin mạng (SOC) cấp bộ, cấp tỉnh…

(4) Tiêu chí 4: *Hệ thống thông tin điều khiển công nghiệp* trực tiếp phục vụ điều khiển, vận hành hoạt động bình thường của các công trình xây dựng cấp II, cấp III hoặc cấp IV theo phân cấp của pháp luật về xây dựng (thực hiện theo hướng dẫn tại Thông tư số 06/2021/TT-BXD ngày 30/6/2021 của Bộ trưởng Bộ Xây dựng quy định về phân cấp công trình xây dựng và hướng dẫn áp dụng trong quản lý hoạt động đầu tư xây dựng).

Ví dụ 3.11. Một số trường hợp điển hình như:

(i) Hệ thống điều khiển phân tán (DCS) các nhà máy thủy điện có tổng công suất lắp máy <=50MW; công trình điện gió/điện mặt trời có tổng công suất <50MW, nhiệt điện có tổng công suất <600MW;

(ii) Hệ thống điều khiển, vận hành trạm biến áp có điện áp <=110kV;

(iii) Hệ thống điều khiển, vận hành nhà máy nước, công trình xử lý nước sạch có tổng công suất <30 nghìn m^3/ngày đêm; trạm bơm nước thô, nước sạch hoặc tăng áp có tổng công suất <40 nghìn m^3/ngày đêm…

5.4. Hệ thống thông tin cấp độ 4

Căn cứ Điều 10 Nghị định số 85/2016/NĐ-CP, hệ thống thông tin cấp độ 4 là hệ thống thông tin có một trong các tiêu chí cụ thể như sau:

(1) Tiêu chí 1: Hệ thống thông tin *xử lý thông tin bí mật nhà nước* hoặc hệ thống phục vụ quốc phòng, an ninh, khi bị phá hoại sẽ làm *tổn hại nghiêm trọng quốc phòng, an ninh quốc gia*.

(2) Tiêu chí 2: *Hệ thống thông tin quốc gia* phục vụ phát triển Chính phủ điện tử, yêu cầu vận hành 24/7 và không chấp nhận ngừng vận hành mà không có kế hoạch trước.

Ví dụ 3.12. Một số trường hợp điển hình như:

(i) Cổng dịch vụ công quốc gia;

(ii) Hệ thống quản lý thuế điện tử, hóa đơn điện tử tập trung;

(iii) Nền tảng tích hợp, chia sẻ dữ liệu quốc gia; Hệ thống định danh và xác thực điện tử quốc gia; Trục liên thông văn bản quốc gia;

(iv) Hệ thống giám sát, đo lường mức độ cung cấp và sử dụng dịch vụ Chính phủ số (Hệ thống EMC); Hệ thống hỗ trợ giám sát, điều hành an toàn mạng phục vụ Chính phủ điện tử (Hệ thống SOC quốc gia)...

(3) Tiêu chí 3: *Hệ thống cơ sở hạ tầng thông tin dùng chung* phục vụ hoạt động của các cơ quan, tổ chức trên phạm vi toàn quốc, yêu cầu vận hành 24/7 và không chấp nhận ngừng vận hành mà không có kế hoạch trước.

Ví dụ 3.13. Một số trường hợp điển hình như:

(i) Hệ thống trung gian thanh toán trực tuyến;

(ii) Các trung tâm dữ liệu, dịch vụ điện toán đám mây cung cấp dịch vụ hạ tầng kỹ thuật cho nhiều cơ quan, tổ chức trên phạm vi toàn quốc, yêu cầu vận hành 24/7 và không chấp nhận ngừng vận hành mà không có kế hoạch trước;

(iii) Các cơ sở dữ liệu quốc gia không thuộc 11 lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng theo Quyết định số 632/QĐ-TTg của Thủ tướng Chính phủ;

(iv) Các cơ sở dữ liệu chuyên ngành phục vụ hoạt động của các cơ quan, tổ chức trên phạm vi toàn quốc, yêu cầu vận hành 24/7 và không chấp nhận ngừng vận hành mà không có kế hoạch trước…

(4) Tiêu chí 4: *Hệ thống thông tin điều khiển công nghiệp* trực tiếp phục vụ điều khiển, vận hành hoạt động bình thường của các công trình xây dựng cấp I theo phân cấp của pháp luật về xây dựng.

Ví dụ 3.14. Một số trường hợp điển hình như:

(i) Hệ thống điều khiển phân tán (DCS) các nhà máy thủy điện có tổng công suất lắp máy >50MW và <=1.000MW; công trình điện gió/điện mặt trời có tổng công suất >=50MW, nhiệt điện có tổng công suất >=600MW và <2.000MW;

(ii) Hệ thống điều khiển, vận hành trạm biến áp có điện áp 220kV;

(iii) Hệ thống điều khiển, vận hành nhà máy nước, công trình xử lý nước sạch có tổng công suất >=30 nghìn m^3/ngày đêm; trạm bơm nước thô, nước sạch hoặc tăng áp có tổng công suất >=40 nghìn m^3/ngày đêm…

5.5. Hệ thống thông tin cấp độ 5

Căn cứ Điều 11 Nghị định số 85/2016/NĐ-CP, hệ thống thông tin cấp độ 5 là hệ thống thông tin có một trong các tiêu chí cụ thể như sau:

(1) Tiêu chí 1: Hệ thống thông tin *xử lý thông tin bí mật nhà nước* hoặc hệ thống phục vụ quốc phòng, an ninh, khi bị phá hoại sẽ làm *tổn hại đặc biệt nghiêm trọng tới quốc phòng, an ninh quốc gia*.

Lưu ý: Việc xác định hệ thống phục vụ quốc phòng, an ninh, khi bị phá hoại sẽ làm *tổn hại, tổn hạn nghiêm trọng hoặc tổn hại đặc biệt nghiêm trọng tới quốc phòng, an ninh quốc gia* thực hiện theo quy hướng dẫn của Bộ Quốc phòng và Bộ Công an.

(2) Tiêu chí 2: Hệ thống thông tin phục vụ lưu trữ dữ liệu tập trung đối với *một số loại hình thông tin, dữ liệu đặc biệt quan trọng của quốc gia*.

Ví dụ 3.15. Điển hình là các hệ thống cơ sở dữ liệu quốc gia thuộc 11 lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng theo Quyết định số 632/QĐ-TTg của Thủ tướng Chính phủ…

(3) Tiêu chí 3: *Hệ thống cơ sở hạ tầng thông tin quốc gia* phục vụ kết nối liên thông hoạt động của Việt Nam với quốc tế.

Ví dụ 3.16. Một số trường hợp điển hình như:

(i) Hệ thống quản lý chuyển mạch quốc tế;

(ii) Hệ thống truyền dẫn và cáp quang biển quốc tế, cáp quang đất liền quốc tế;

(iii) Hệ thống thanh toán qua SWIFT phục vụ thanh toán quốc tế…

(4) Tiêu chí 4: *Hệ thống thông tin điều khiển công nghiệp* trực tiếp phục vụ điều khiển, vận hành hoạt động bình thường của công trình xây dựng cấp đặc biệt theo phân cấp của pháp luật về xây dựng hoặc công trình quan trọng liên quan đến an ninh quốc gia theo pháp luật về an ninh quốc gia.

Ví dụ 3.17. Một số trường hợp điển hình như:

(i) Hệ thống điều khiển phân tán (DCS) các nhà máy thủy điện có tổng công suất lắp máy >1.000MW; công trình nhiệt điện có tổng công suất >2.000MW; công trình điện hạt nhân;

(ii) Hệ thống điều khiển, vận hành trạm biến áp có điện áp >=500kV…

(5) Tiêu chí 5: Hệ thống thông tin khác do Thủ tướng Chính phủ quyết định.

Ví dụ 3.18. Một số trường hợp điển hình như:

(i) Mạng truyền số liệu chuyên dùng phục vụ các cơ quan Đảng, Nhà nước;

(ii) Hệ thống quản lý văn bản 4 cấp chính quyền;

(iii) Hệ thống máy chủ tên miền quốc gia Việt Nam ".vn";

(iv) Hệ thống quản lý, điều khiển, khai thác, vận hành vệ tinh viễn thông hoặc mạng đường trục băng rộng…

TỔNG KẾT CHƯƠNG 3

1. Việc xác định cấp độ an toàn thông tin của hệ thống thông tin phải được thực hiện trên cơ sở ***xác định chính xác***:

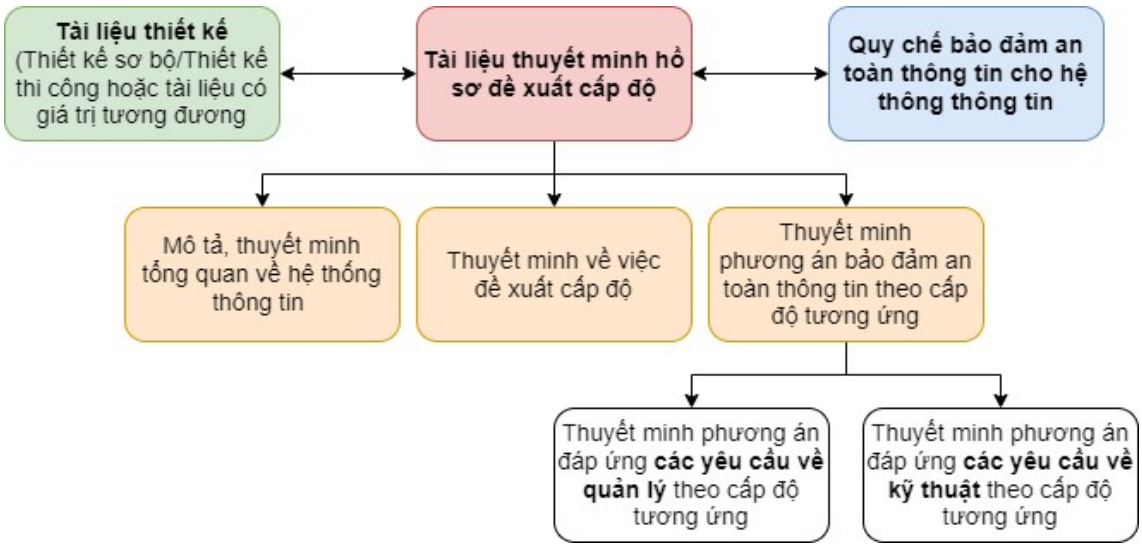
- ❖ Các loại thông tin mà hệ thống thông tin xử lý (theo quy định tại khoản 1 Điều 6 Nghị định số 85/2016/NĐ-CP);
- ❖ Loại hình hệ thống thông tin (theo quy định tại khoản 2 Điều 6 Nghị định số 85/2016/NĐ-CP);
- ❖ Tiêu chí xác định cấp độ (theo quy định tại các Điều 7, 8, 9, 10 và 11 Nghị định số 85/2016/NĐ-CP).

Đây là cơ sở để triển khai các biện pháp cơ bản (tối thiểu) bảo đảm an toàn thông tin về mặt quản lý và kỹ thuật phù hợp với cấp độ đề xuất.

2. Việc ***xác định sai cấp độ đề xuất*** dẫn đến triển khai các biện pháp bảo đảm an toàn thông tin không phù hợp có thể gây ra nguy cơ mất an toàn thông tin đối với hệ thống thông tin (nếu đề xuất ở cấp độ thấp hơn so với quy định của pháp luật) hoặc gây ra hậu quả đầu tư lãng phí cho Ngân sách nhà nước (nếu đề xuất ở cấp độ cao hơn so với quy định của pháp luật).

Chương 4.
Xây dựng hồ sơ đề xuất cấp độ

Hồ sơ đề xuất cấp độ an toàn hệ thống thông tin là cơ sở để triển khai các biện pháp bảo đảm an toàn thông tin theo quy định, là căn cứ quan trọng để xác định và bố trí nguồn lực triển khai cũng như đánh giá mức độ tuân thủ pháp luật về an toàn thông tin mạng.



Hình 4. Các thành phần của hồ sơ đề xuất cấp độ an toàn thông tin.

Căn cứ quy định tại Điều 15 Nghị định số 85/2016/NĐ-CP và khoản 2 Điều 8 Thông tư số 12/2022/TT-BTTTT, hồ sơ đề xuất cấp độ bao gồm:

(1) Tài liệu thiết kế hệ thống thông tin: Tùy thuộc vào hình thức đầu tư, tài liệu thiết kế hệ thống thông tin là một trong các tài liệu sau đây:

- Đối với dự án đầu tư xây dựng mới hoặc mở rộng, nâng cấp hệ thống thông tin: 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;

- Đối với hệ thống thông tin đang vận hành: Báo cáo kinh tế - kỹ thuật hoặc thiết kế chi tiết hoặc kế hoạch thuê dịch vụ công nghệ thông tin hoặc đề cương và dự toán chi tiết đã được phê duyệt;

(2) Tài liệu thuyết minh hồ sơ đề xuất cấp độ gồm các thành phần sau đây:

- Mô tả, thuyết minh tổng quan về hệ thống thông tin;

- Thuyết minh về việc đề xuất cấp độ;

- Thuyết minh phương án bảo đảm an toàn thông tin theo cấp độ tương ứng;

(3) Quy chế bảo đảm an toàn thông tin cho hệ thống thông tin.

Mẫu hồ sơ đề xuất cấp độ được đăng tải trên Nền tảng hỗ trợ quản lý bảo đảm an toàn hệ thống thông tin theo cấp độ, tại địa chỉ https://capdo.ais.gov.vn.

Chương này sẽ hướng dẫn chi tiết cách thức xây dựng hồ sơ đề xuất cấp độ và quy chế bảo đảm an toàn thông tin cho hệ thống thông tin.

1. Khi nào cần xây dựng hồ sơ đề xuất cấp độ?

Căn cứ quy định tại các Điều 13, 14 và 18 Nghị định số 85/2016/NĐ-CP, khoản 1 Điều 8 Thông tư số 12/2022/TT-BTTTT, đối với các hệ thống thông tin thuộc phạm vi điều chỉnh của Nghị định số 85/2016/NĐ-CP, các trường hợp sau đây cần được xây dựng hoặc phải tiến hành rà soát, điều chỉnh, bổ sung, hoàn thiện hồ sơ đề xuất cấp độ, cụ thể:

a) Ngay sau khi được cấp có thẩm quyền phê duyệt chủ trương xây dựng mới hoặc nâng cấp mở rộng hệ thống thông tin và chủ đầu tư/đơn vị chủ trì thuê dịch vụ tiến hành xây dựng tài liệu thiết kế hệ thống thông tin, là 01 trong các tài liệu báo cáo kinh tế - kỹ thuật (trong trường hợp dự án đầu tư áp dụng phương án thiết kế 01 bước) hoặc thiết kế cơ sở thuộc báo cáo nghiên cứu khả thi (trong trường hợp dự án đầu tư áp dụng phương án thiết kế 02 bước) hoặc kế hoạch thuê dịch vụ công nghệ thông tin (trong trường hợp áp dụng hình thức thuê dịch vụ công nghệ thông tin) hoặc đề cương và dự toán chi tiết (trong trường hợp đầu tư ứng dụng công nghệ thông tin không phải lập dự án theo quy định):

- Xây dựng song song hồ sơ đề xuất cấp độ an toàn thông tin với tài liệu thiết kế hệ thống thông tin;

- Đồng bộ nội dung thuyết minh trong hồ sơ đề xuất cấp độ với phương án kỹ thuật trong dự thảo báo cáo kinh tế - kỹ thuật hoặc dự thảo thiết kế cơ sở thuộc báo cáo nghiên cứu khả thi hoặc dự thảo kế hoạch thuê dịch vụ công nghệ thông tin hoặc dự thảo đề cương và dự toán chi tiết tương ứng.

b) Hệ thống thông tin đang vận hành nhưng chưa được phê duyệt cấp độ an toàn thông tin:

Xây dựng hồ sơ đề xuất cấp độ an toàn thông tin cho hệ thống thông tin, đồng bộ với phương án kỹ thuật trong báo cáo kinh tế - kỹ thuật hoặc thiết kế chi tiết hoặc kế hoạch thuê dịch vụ công nghệ thông tin hoặc đề cương và dự toán chi tiết tương ứng đã được phê duyệt.

c) Hệ thống thông tin đang vận hành đã được phê duyệt cấp độ nhưng được cập nhật, mở rộng hoặc qua rà soát thấy cần phải điều chỉnh, bổ sung, hoàn thiện hồ sơ đề xuất cấp độ (điều chỉnh cấp độ hoặc điều chỉnh các phương án bảo đảm an toàn thông tin):

Cần tiến hành rà soát, điều chỉnh, bổ sung, hoàn thiện nội dung hồ sơ đề xuất cấp độ cho phù hợp, đồng bộ với phương án kỹ thuật được phê duyệt hoặc được cập nhật, mở rộng.

Lưu ý:

(1) Việc xây dựng, điều chỉnh, cập nhật, hoàn thiện hồ sơ đề xuất cấp độ do đơn vị vận hành hệ thống thông tin chủ trì thực hiện. Đối với trường hợp a ở

trên, trong giai đoạn này, chủ đầu tư đóng vai trò là đơn vị vận hành hệ thống thông tin;

(2) Để việc xây dựng hồ sơ đề xuất cấp độ cho hệ thống thông tin được hiệu quả, chất lượng, đáp ứng các yêu cầu đề ra, chủ đầu tư/đơn vị vận hành hệ thống thông tin cần tổ chức khảo sát tổng thể thiết kế hệ thống và hiện trạng hạ tầng kỹ thuật dự kiến phục vụ triển khai hệ thống trên cơ sở các quy định tại Điều 19 Nghị định số 85/2016/NĐ-CP; Điều 9, Điều 10 và Phụ lục tương ứng với cấp độ đề xuất được ban hành kèm theo Thông tư số 12/2022/TT-BTTTT, để từ đó thuyết minh hồ sơ đề xuất cấp độ và đề xuất cách thức triển khai các phương án bảo đảm an toàn thông tin theo cấp độ tương ứng cho phù hợp.

2. Lồng ghép thuyết minh đề xuất cấp độ vào tài liệu thiết kế hệ thống thông tin

Việc xây dựng nội dung thuyết minh đề xuất cấp độ, lồng ghép vào tài liệu thiết kế hệ thống thông tin theo quy định tại Điều 13 Nghị định số 85/2016/NĐ-CP phải đảm bảo:

(1) Thuyết minh đề xuất cấp độ trong tài liệu thiết kế hệ thống thông tin phù hợp với nội dung đề xuất cấp độ được thuyết minh trong hồ sơ đề xuất cấp độ an toàn thông tin của hệ thống thông tin;

(2) Thuyết minh phương án kỹ thuật trong tài liệu thiết kế hệ thống thông tin phải đồng bộ, đáp ứng các yêu cầu của phương án bảo đảm an toàn thông tin theo cấp độ được thuyết minh trong hồ sơ đề xuất cấp độ, trong đó, tối thiểu phải thuyết minh đồng bộ, làm rõ các nội dung sau đây: (i) mô hình kiến trúc hệ thống bao gồm mô hình lô-gic và mô hình vật lý; (ii) các yêu cầu, đề xuất về hạ tầng kỹ thuật gồm các thiết bị mạng, các máy chủ, các thiết bị và giải pháp bảo đảm an toàn thông tin cần triển khai.

Bên cạnh đó, căn cứ các quy định tại khoản 8 Điều 9 Thông tư số 12/2022/TT-BTTTT, yêu cầu bảo đảm an toàn thông tin đối với phần mềm nội bộ khi xây dựng mới hoặc mở rộng, nâng cấp phải tuân thủ Khung phát triển phần mềm an toàn và đáp ứng yêu cầu an toàn cơ bản đối với Phần mềm nội bộ. Do đó, trong quá trình thiết kế, các yêu cầu, chức năng của phần mềm nội bộ trong tài liệu thiết kế hệ thống thông tin cần đảm bảo:

- Tuân thủ hướng dẫn "Khung phát triển phần mềm an toàn (phiên bản 1.0)" được Cục An toàn thông tin ban hành tại Văn bản số 166/CATTT-ATHTTT ngày 10/02/2022, và;

- Đáp ứng yêu cầu an toàn cơ bản đối với Phần mềm nội bộ được Bộ trưởng Bộ Thông tin và Truyền thông ban hành tại Quyết định số 742/QĐ-BTTTT ngày 22/4/2022.

3. Thuyết minh tổng quan về hệ thống thông tin

Căn cứ quy định tại khoản 3 Điều 8 Thông tư số 12/2022/TT-BTTTT, thuyết minh tổng quan về hệ thống thông tin bao gồm các nội dung sau đây:

3.1. Thông tin về chủ quản hệ thống thông tin

Thông tin về chủ quản hệ thống thông tin, gồm:

(1) Tên chủ quản hệ thống thông tin: Ghi rõ tên cơ quan được xác định là chủ quản hệ thống thông tin;

(2) Quy định chức năng, nhiệm vụ và quyền hạn: Ghi rõ thông tin văn bản quy định chức năng, nhiệm vụ và quyền hạn (nếu có) của cơ quan được xác định là chủ quản hệ thống thông tin. Trường hợp không có thì để trống;

(3) Người đại diện, chức vụ: Ghi rõ họ và tên, chức vụ của người đứng đầu cơ quan được xác định là chủ quản hệ thống thông tin;

(4) Địa chỉ liên lạc của cơ quan được xác định là chủ quản hệ thống thông tin;

(5) Thông tin liên hệ bao gồm: Số điện thoại, thư điện tử của cơ quan được xác định là chủ quản hệ thống thông tin.

Trường hợp có ủy quyền trách nhiệm của chủ quản hệ thống thông tin thì bên cạnh thông tin về chủ quản hệ thống thông tin cần bổ sung các thông tin về văn bản ủy quyền, đơn vị được ủy quyền, phạm vi, thời gian ủy quyền.

3.2. Thông tin về đơn vị vận hành hệ thống thông tin

Thông tin về đơn vị vận hành hệ thống thông tin, gồm:

(1) Tên đơn vị vận hành: Ghi rõ tên cơ quan/đơn vị được chủ quản hệ thống thông tin giao là đơn vị vận hành hệ thống thông tin;

(2) Quy định chức năng, nhiệm vụ và quyền hạn: Ghi rõ thông tin văn bản quy định chức năng, nhiệm vụ và quyền hạn (nếu có) của đơn vị vận hành hệ thống thông tin. Trường hợp không có thì để trống;

(3) Người đại diện, chức vụ: Ghi rõ họ và tên, chức vụ của người đứng đầu cơ quan được chủ quản hệ thống thông tin giao là đơn vị vận hành hệ thống thông tin;

(4) Địa chỉ liên lạc của cơ quan được chủ quản hệ thống thông tin giao là đơn vị vận hành hệ thống thông tin;

(5) Thông tin liên hệ bao gồm: Số điện thoại, thư điện tử của cơ quan được chủ quản hệ thống thông tin giao là đơn vị vận hành hệ thống thông tin.

3.3. Mô tả phạm vi, quy mô của hệ thống thông tin

Làm rõ phạm vi, quy mô và các đối tượng phục vụ của hệ thống, đồng bộ với nội dung phạm vi, quy mô và các đối tượng phục vụ của hệ thống thông tin thuộc tài liệu thiết kế hệ thống thông tin.

3.4. Mô tả kiến trúc hệ thống

Phần này 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:

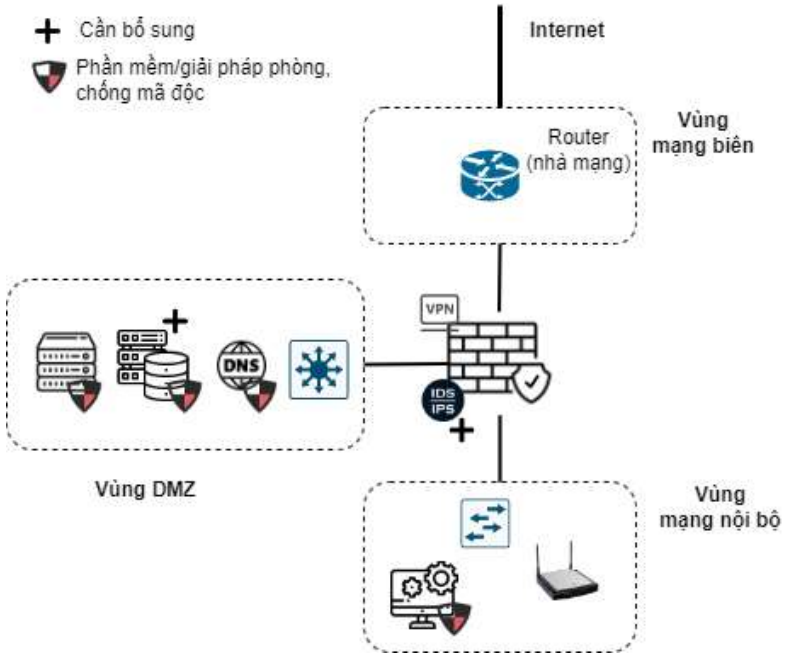
3.4.1. Mô hình lô-gic của hệ thống

Khái niệm: *Mô hình lô-gic của hệ thống thông tin*[25] là mô hình thể hiện mức chi tiết của mô hình tổng thể. Mô hình lô-gic thể hiện quy trình xử lý giữa các thành phần của hệ thống hoặc giữa hệ thống với các hệ thống khác có liên quan để giải quyết các yêu cầu kỹ thuật của hệ thống đó nhằm đưa ra các kết quả mong muốn.

Yêu cầu tối thiểu: Thể hiện rõ thiết kế các vùng mạng của hệ thống theo chức năng và các phương án bảo đảm an toàn thông tin bảo vệ các vùng mạng, phù hợp với yêu cầu cơ bản bảo đảm an toàn hệ thống thông tin được ban hành tại Phụ lục tương ứng với cấp độ đề xuất của Thông tư số 12/2022/TT-BTTTT.

Ví dụ 4.1. Mô hình lô-gic tham khảo:

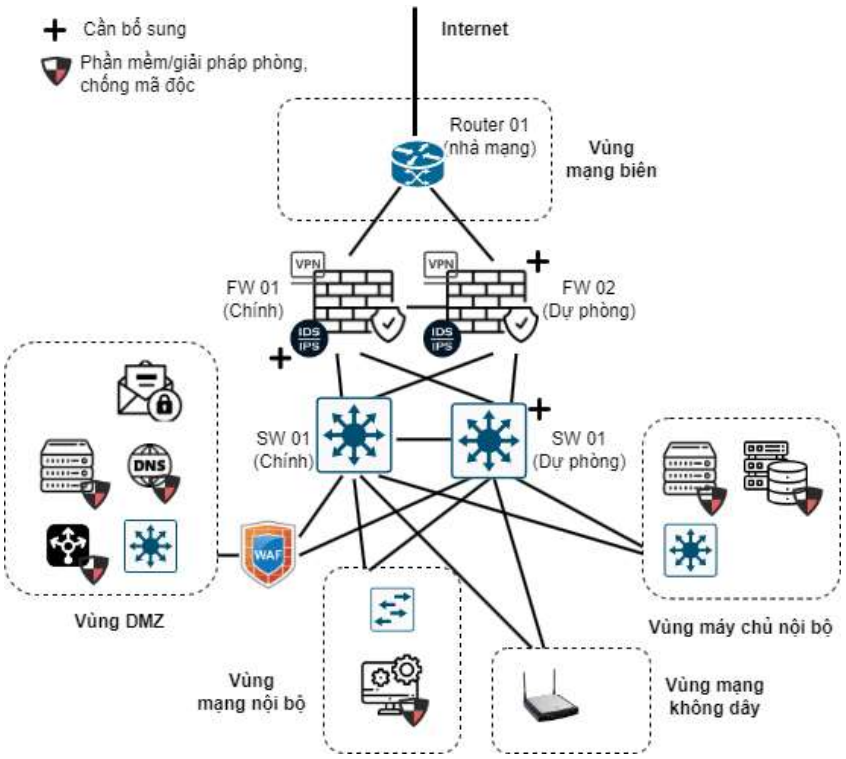
(i) Đối với hệ thống thông tin cấp độ 1:



Hình 5. Mô hình lô-gic tham khảo đối với hệ thống thông tin cấp độ 1

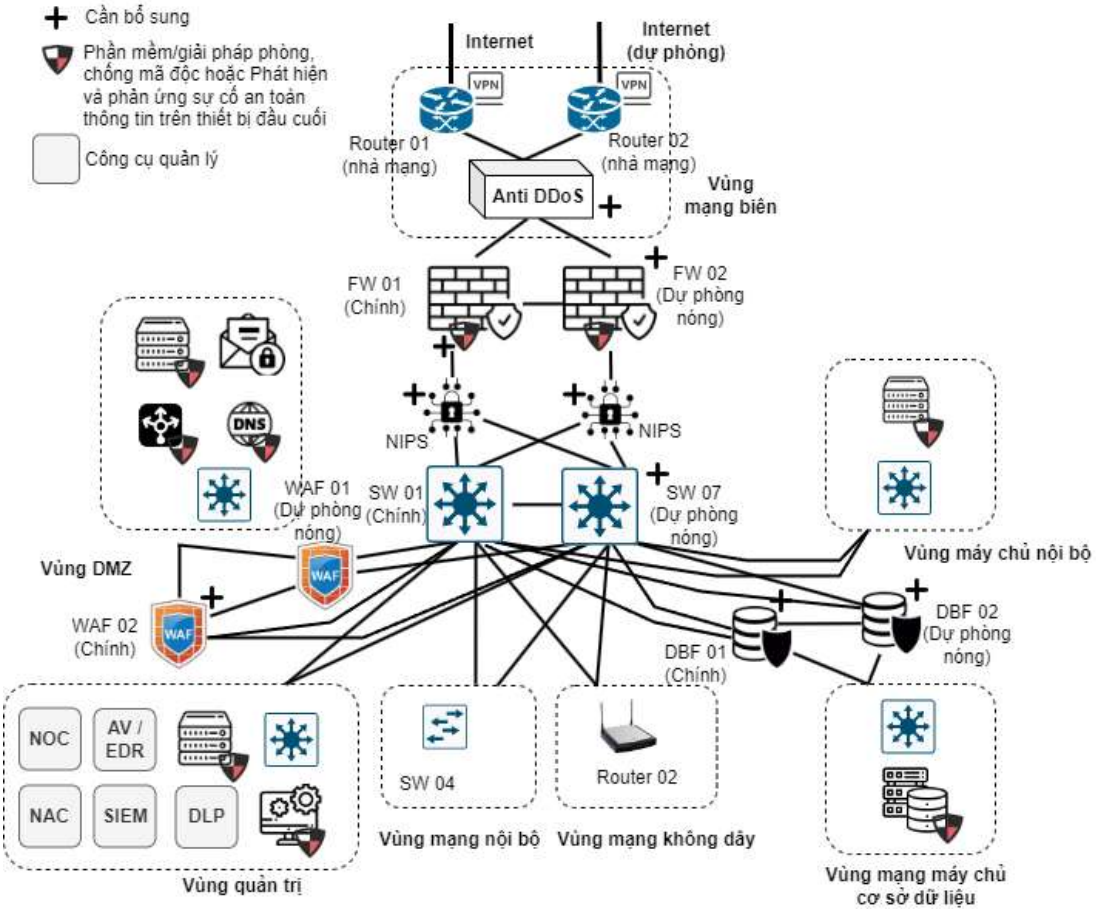
(ii) Đối với hệ thống thông tin cấp độ 2:

[25] Khoản 22 Điều 3 Nghị định số 73/2019/NĐ-CP.



Hình 6. Mô hình lô-gic tham khảo đối với hệ thống thông tin cấp độ 2

(iii) Đối với hệ thống thông tin cấp độ 3:



Hình 7. Mô hình lô-gic tham khảo đối với hệ thống thông tin cấp độ 3

Lưu ý:

(1) Bên cạnh việc đảm bảo các yêu cầu tối thiểu theo cấp độ đề xuất, thiết kế hệ thống cũng cần phù hợp với mục đích, chức năng, phạm vi, đối tượng phục vụ. Do đó, có thể không áp dụng một hoặc một số các vùng mạng và giải pháp an toàn thông tin tương ứng được yêu cầu nhưng cần có thuyết minh làm rõ lý do không áp dụng. Chẳng hạn, hệ thống thông tin cấp độ 2 chỉ hoạt động trong vùng mạng nội bộ của cơ quan, đơn vị có thể không cần thiết kế vùng DMZ và tương ứng không cần đầu tư giải pháp phòng chống tấn công mạng cho ứng dụng web;

(2) Trường hợp hiện trạng hạ tầng kỹ thuật phục vụ triển khai, vận hành hệ thống chưa đáp ứng yêu cầu bảo đảm an toàn thông tin theo cấp độ được đề xuất thì cần làm rõ mô tả hiện trạng kiến trúc hệ thống và mô tả kiến trúc hệ thống cần thiết kế để đáp ứng yêu cầu. Khi đó:

- Có thể thể hiện thông qua hai mô hình riêng biệt hoặc thể hiện chung trong cùng một mô hình (như **Ví dụ 4.1**);

- Cần làm rõ các thiết bị mạng, máy chủ, thiết bị/giải pháp an toàn thông tin cần bổ sung, như các thành phần được đánh dấu (+) trong **Ví dụ 4.1** ở trên. Đây chính là các thành phần được xác định phải sớm đầu tư bổ sung để đảm bảo hệ thống thông tin được vận hành an toàn, đáp ứng yêu cầu bảo đảm an toàn thông tin theo cấp độ đề xuất;

(3) Sau khi đã hoàn thành việc đầu tư bổ sung các thiết bị mạng, máy chủ, thiết bị/giải pháp an toàn thông tin đáp ứng yêu cầu thì cần cập nhật, hoàn thiện hồ sơ đề xuất cấp độ theo đúng hiện trạng thực tế.

Danh sách các phân vùng mạng tối thiểu:

STT	Vùng mạng[26]	Cấp độ				
		1	2	3	4	5
1	*Vùng mạng biên* (outside zone hay Internet zone) là vùng mạng được thiết lập để cung cấp các kết nối hệ thống ra bên ngoài Internet và các mạng khác.	x	x	x	x	x
2	*Vùng mạng nội bộ* (LAN - local area network hay users zone) là vùng mạng được thiết lập để cung cấp kết nối mạng cho các máy trạm và các thiết bị đầu cuối và các thiết bị khác của người sử dụng vào hệ thống.	x	x	x	x	x
3	*Vùng DMZ* (demilitarized zone) là vùng mạng được thiết lập để đặt các máy chủ công cộng, cho phép truy cập trực tiếp từ các mạng bên ngoài và mạng Internet	x	x	x	x	x
4	*Vùng máy chủ nội bộ* (internal server zone hay servers		x	x	x	x

[26] Theo Tiêu chuẩn quốc gia TCVN 11930:2017.

	farm) là vùng mạng được thiết lập để đặt các máy chủ nội bộ, cung cấp các ứng dụng, dịch vụ phục vụ hoạt động nội bộ của tổ chức và các hoạt động khác mà không cho phép truy cập trực tiếp từ các mạng bên ngoài.					
5	*Vùng mạng không dây* hay vùng wifi.		x	x	x	x
6	*Vùng máy chủ cơ sở dữ liệu* (database server zone) là vùng mạng được thiết lập để đặt các máy chủ cơ sở dữ liệu. Các máy chủ trong vùng này được triển khai tách biệt với các máy chủ ứng dụng nhằm tăng cường các biện kiểm soát truy cập giữa các vùng máy chủ khác với vùng máy chủ này.			x	x	x
7	*Vùng quản trị* (management zone) là vùng mạng được thiết lập để đặt các máy chủ, máy quản trị và các thiết bị chuyên dụng khác phục vụ việc quản lý, vận hành và giám sát hệ thống.			x	x	x
8	*Vùng quản trị thiết bị hệ thống* (device management zone) là vùng mạng riêng cho các địa chỉ quản trị của các thiết bị hệ thống cho phép thiết lập chính sách chung và quản lý tập trung các thiết bị hệ thống.				x	x

Bảng 1. Danh sách các phân vùng mạng tối thiểu.

3.4.2. Mô hình vật lý của hệ thống:

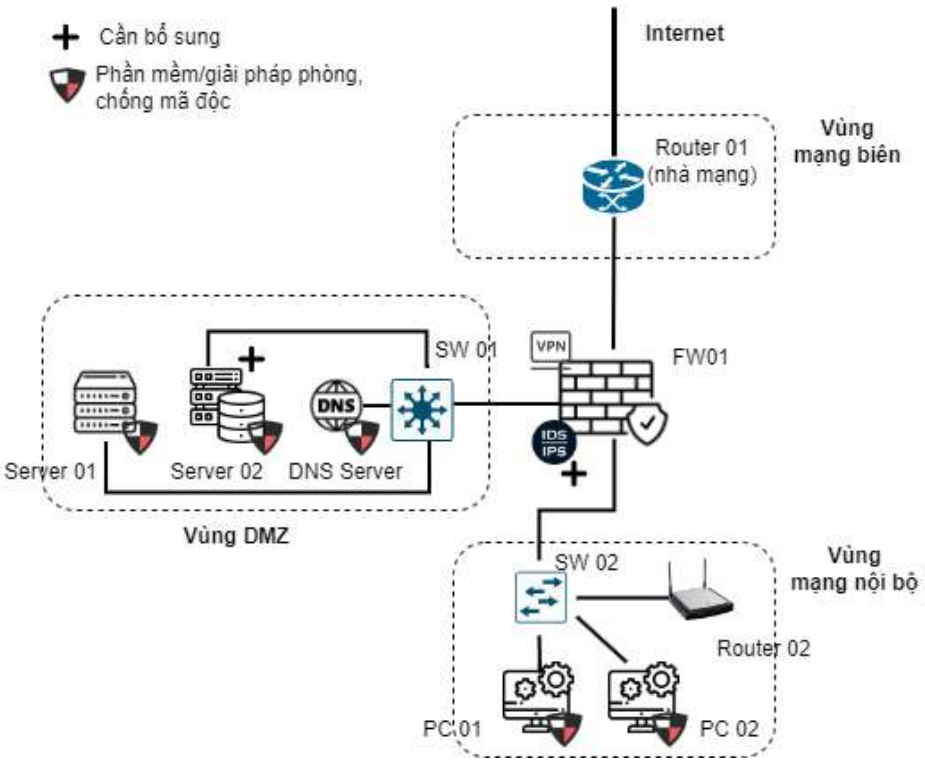
Khái niệm: *Mô hình vật lý của hệ thống thông tin*[27] là mô hình thể hiện mức chi tiết của mô hình lô-gic. Mô hình này biểu diễn thiết kế của hệ thống thông tin dựa trên mô hình lô-gic và giải pháp thiết kế của hệ thống đã được lựa chọn với các thông tin về giải pháp, thông số kỹ thuật và thiết bị, công cụ sử dụng (nếu có) phù hợp với tiêu chuẩn, quy chuẩn kỹ thuật được áp dụng.

Yêu cầu tối thiểu: Thể hiện rõ kết nối giữa các thiết bị mạng, máy chủ, thiết bị an toàn thông tin, phù hợp với mô hình lô-gic. Trường hợp hạ tầng kỹ thuật phục vụ triển khai, vận hành hệ thống sử dụng các máy chủ ảo thì cần có chú thích, làm rõ các vùng mạng, máy chủ ảo, giải pháp an toàn thông tin được tạo hoặc cài đặt lập trên các máy chủ vật lý nào.

Ví dụ 4.2. Mô hình vật lý tham khảo:

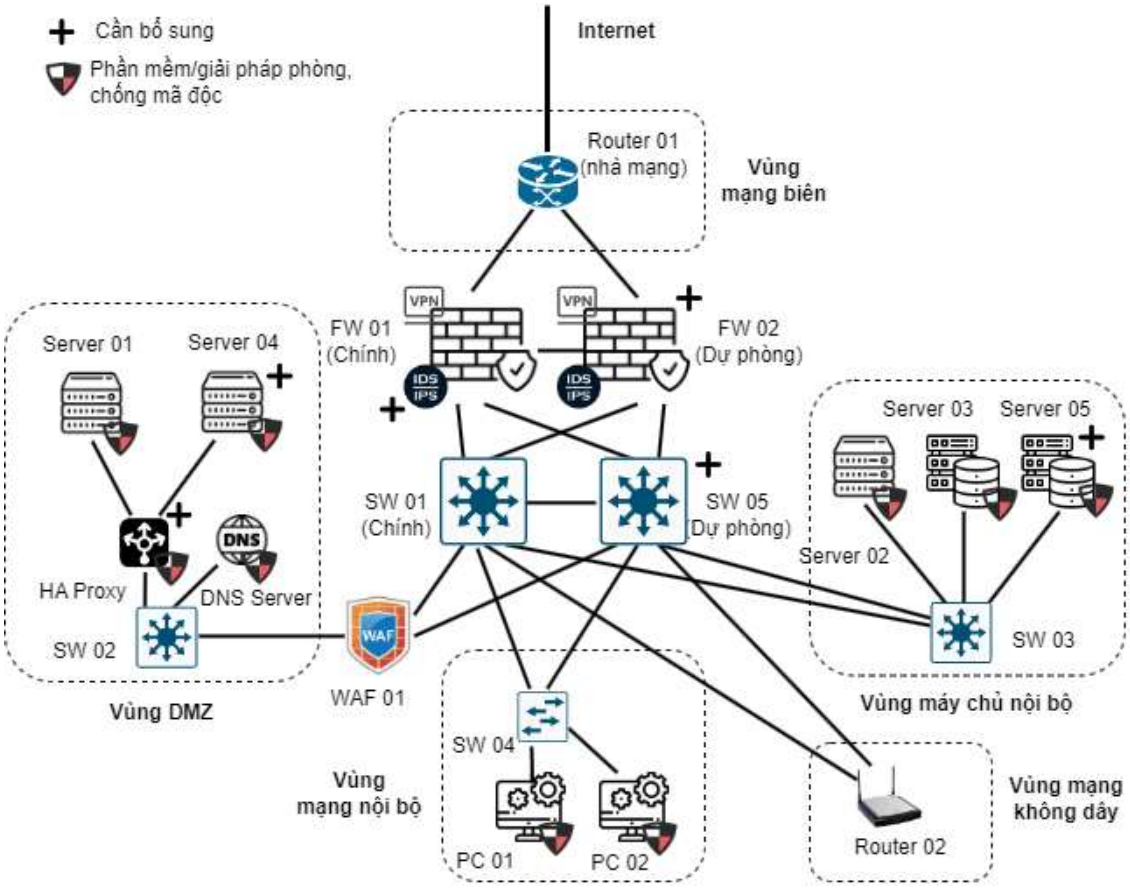
(i) Đối với hệ thống thông tin cấp độ 1: Mô hình này tương ứng với mô hình lô-gic trong **Ví dụ 4.1** ở trên.

[27] Khoản 23 Điều 3 Nghị định số 73/2019/NĐ-CP.



Hình 8. Mô hình vật lý tham khảo đối với hệ thống thông tin cấp độ 1

(ii) Đối với hệ thống thông tin cấp độ 2: Mô hình này tương ứng với mô hình lô-gic trong **Ví dụ 4.1** ở trên.



Hình 9. Mô hình vật lý tham khảo đối với hệ thống thông tin cấp độ 2

Lưu ý: Mô tả về mô hình lô-gic, mô hình vật lý của hệ thống thông tin phải được thuyết minh đồng bộ với mô hình kiến trúc tổng thể, mô hình lô-gic, mô hình vật lý của hệ thống thuộc tài liệu thiết kế hệ thống thông tin.

3.4.3. Danh mục thiết bị và thiết bị mạng chính trong hệ thống (thuyết minh dưới dạng bảng)

STT	Tên thiết bị/chủng loại[28]	Vị trí triển khai[29]	Mục đích sử dụng
1	Firewall FW01[30] Fortigate 40F	Vùng thiết bị trung tâm	- Tường lửa trung tâm, bảo vệ toàn bộ hệ thống hạ tầng mạng phục vụ triển khai hệ thống. Hiện bảo vệ ở mức cơ bản; đã tích hợp tính năng VP nhưng chưa có tính năng quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập; - Là thiết bị mạng chính.
2	Router 01	Vùng mạng biên	Thiết bị router do nhà mạng cung cấp dịch vụ Internet cung cấp
3	Switch SW 01 TP-LINK TL-SG1008MP	Vùng DMZ	
4	Switch SW 02 TP-LINK TL-SG1008MP	Vùng mạng nội bộ	
5	Router 02 TP Link Archer AX73	Vùng mạng nội bộ	Phục vụ phát Internet cho các máy tính hoặc thiết bị mạng có kết nối không dây. Tuy nhiên không được cấu hình để truy cập vào các máy chủ tại Vùng DMZ
6	PC 01: xxx-204, IP: 192.168.3.192[31]	Vùng mạng nội bộ	Máy tính của quản trị viên hệ thống, đặt tại phòng quản trị, trong vùng mạng LAN. Được sử dụng để kết nối, giám

[28] Liệt kê các thiết bị mạng, thiết bị an toàn thông tin, thiết bị đầu cuối (PC, laptop, camera giám sát được triển khai ở các phân vùng mạng tham gia điều hướng mạng, vận hành hoặc bảo đảm an toàn thông tin cho hệ thống thông tin.
[29] Chỉ rõ vùng mạng phục vụ triển khai.
[30] Thông tin được thuyết minh trong Bảng 2, 3, 4 là **ví dụ minh họa** ứng với mô hình vật lý tại Hình 8.
[31] Chỉ rõ địa chỉ IP hoặc tên định danh của các thiết bị/máy chủ để thuận tiện trong việc quản lý, rà soát khi cần.

			sát, fix bug trên các máy chủ triển khai hệ thống.
7	PC 02: xxx-206, IP: 192.168.3.112	Vùng mạng nội bộ	Máy tính của quản trị viên hệ thống, đặt tại phòng quản trị, trong vùng mạng LAN. Được sử dụng để kết nối, giám sát, fix bug trên các máy chủ triển khai hệ thống.
8	*[Các thiết bị mạng, thiết bị đầu cuối khác, nếu có]*	…	*[Ghi rõ mục đích sử dụng của thiết bị và xác định thiết bị có được được xem là thiết bị mạng chính hay không để làm căn cứ đầu tư dự phòng cho phù hợp]*

Bảng 2. Danh mục thiết bị trong hệ thống

Thiết bị mạng chính hoặc quan trọng[32] 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.

3.4.4. Danh mục ứng dụng/dịch vụ cung cấp bởi hệ thống (thuyết minh dưới dạng bảng)

STT	**Tên ứng dụng/dịch vụ**[33]	**Máy chủ triển khai**[34]	**Vị trí triển khai**[35]	**Hệ điều hành máy chủ**	**Mục đích sử dụng**[36]
1	Dịch vụ DNS	DNS Server 192.168.10.10	Vùng DMZ	Windows Server 2022	Dịch vụ hạ tầng, dùng để phân giải tên miền về máy chủ ứng dụng web trong vùng DMZ.

[32] Khoản 2 Điều 3 Thông tư số 12/2022/TT-BTTTT.

[33] Ghi tên các ứng dụng phần mềm hoặc dịch vụ công nghệ thông tin **(các ứng dụng/dịch vụ có domain truy cập riêng)** được cung cấp bởi hệ thống thông tin chính và các hệ thống thông tin thành phần hoặc **các dịch vụ hạ tầng có ảnh hưởng trực tiếp đến hoạt động bình thường của hệ thống (như dịch vụ DNS)**.

[34] Liệt kê các máy chủ phục vụ triển khai hệ thống hoặc phân nhóm theo từng ứng dụng/dịch vụ. Danh sách máy chủ phải khớp với các máy chủ được mô tả trong mô hình vật lý.

[35] Chỉ rõ vùng mạng phục vụ triển khai.

[36] Làm rõ máy chủ phục vụ mục đích gì, triển khai cho hệ thống thông tin thành phần nào hoặc ứng dụng/dịch vụ cụ thể nào. Trường hợp máy chủ này hiện tại chưa có thì ghi theo chủng loại và làm rõ cần đầu tư mới, dự kiến lộ trình đầu tư.

2	*[Ví dụ: Trang thông tin điện tử của Ủy ban nhân dân huyện X]*	Server 01, IP: 192.168.10.22	Vùng DMZ	Windows Server 2022	Cài đặt ứng dụng web của trang thông tin điện tử. Hiện tại đang được dùng để cài đặt cả cơ sở dữ liệu của trang thông tin điện tử, tuy nhiên không bảo đảm hiệu năng và an toàn.
		Server 02, IP: 192.168.10.32 (dự kiến)	Vùng DMZ	CentOS 7	Cài đặt cơ sở dữ liệu của ứng dụng. Hiện trạng: Chưa có, cần đầu tư trước tháng … năm 2024 để bảo đảm kế hoạch triển khai hệ thống[37].
2	…	*[Các máy chủ khác nếu có]*	Vùng DMZ	…	…

Bảng 3. Danh mục ứng dụng/dịch vụ cung cấp bởi hệ thống

3.4.5. Quy hoạch các vùng mạng và địa chỉ IP trong hệ thống (thuyết minh dưới dạng bảng)

STT	Vùng mạng	Địa chỉ IP nội bộ (IP Private)	Địa chỉ IP công khai (IP Public)
1	Vùng DMZ	192.168.10.0/24	202.191.z.0/24
2	Vùng mạng nội bộ	192.168.3.0/24	//[38]

Bảng 4. Quy hoạch các vùng mạng và địa chỉ IP trong hệ thống

4. Thuyết minh về việc đề xuất cấp độ

Căn cứ quy định tại khoản 4 Điều 8 Thông tư số 12/2022/TT-BTTTT, thuyết minh về việc đề xuất cấp độ bao gồm các nội dung sau đây:

[37] Lưu ý: Sau khi được bổ sung, cần cập nhật lại thông tin cho phù hợp.
[38] Trường hợp không public ra Internet ghi "//".

4.1. Danh mục các hệ thống thông tin và cấp độ tương ứng

STT	Tên hệ thống thông tin	Cấp độ đề xuất	Căn cứ đề xuất cấp độ
1	[Tên hệ thống thông tin chính. Ví dụ: Trang thông tin điện tử của Ủy ban nhân dân huyện X]	1	Điều 7 Nghị định số 85/2016/NĐ-CP.
2	[Tên hệ thống thông tin thành phần 01 (nếu có)]	1	Điều 7 Nghị định số 85/2016/NĐ-CP.
3	[Tên hệ thống thông tin thành phần 02 (nếu có)]	1	Điều 7 Nghị định số 85/2016/NĐ-CP.
4	…	…	…

Bảng 5. Danh mục các hệ thống thông tin và cấp độ tương ứng

Căn cứ nguyên tắc xác định cấp độ được quy định tại khoản 2 Điều 5 Nghị định số 85/2016/NĐ-CP, trong trường hợp hệ thống thông tin chính bao gồm nhiều hệ thống thành phần và mỗi hệ thống thành phần lại tương ứng với một cấp độ khác nhau thì cấp độ an toàn thông tin của hệ thống thông tin chính *được xác định là cấp độ cao nhất* trong các cấp độ an toàn thông tin của các hệ thống thành phần cấu thành nên hệ thống thông tin chính. Do đó:

(1) Trường hợp nếu hệ thống thông tin chính không có các hệ thống thông tin thành phần thì bảng danh mục các hệ thống thông tin và cấp độ tương ứng chỉ để lại dòng mô tả về hệ thống thông tin chính;

(2) Trường hợp hệ thống thông tin chính được đề xuất cấp độ 1 thì các hệ thống thông tin thành phần (nếu có) cũng được đề xuất cấp độ 1.

Khuyến khích **các hệ thống thông tin có nghiệp vụ độc lập được xây dựng hồ sơ đề xuất cấp độ riêng** để thuận tiện trong việc thuyết minh rõ các thiết bị mạng, máy chủ, thiết bị và giải pháp an toàn thông tin tham gia phục vụ vận hành hệ thống thông tin. Bên cạnh đó, trong trường hợp cần nâng cấp, mở rộng hệ thống thông tin, việc điều chỉnh hồ sơ đề xuất cấp độ của một hệ thống thông tin cụ thể không ảnh hưởng đến hồ sơ đề xuất cấp độ của các hệ thống thông tin khác.

4.2. Thuyết minh chi tiết đối với các hệ thống thông tin

Thuyết minh chi tiết đề xuất cấp độ an toàn thông tin đối với từng hệ thống thông tin cần làm rõ:

(1) Loại thông tin được hệ thống thông tin xử lý (khoản 1 Điều 6 Nghị định số 85/2016/NĐ-CP);

(2) Loại hình của hệ thống thông tin (khoản 2 Điều 6 Nghị định số 85/2016/NĐ-CP);

(3) Căn cứ đề xuất cấp độ (Điều 7, Điều 8, Điều 9, Điều 10 và Điều 11 Nghị định số 85/2016/NĐ-CP).

Nội dung thuyết minh cần chi tiết, cụ thể và đồng bộ với các nội dung về phạm vi, quy mô và đối tượng phục vụ của hệ thống đã được thuyết minh trong tài liệu thiết kế và phần thuyết minh tổng quan trong hồ sơ đề xuất cấp độ.

Ví dụ 4.3. Thuyết minh chi tiết đề xuất cấp độ đối với Trang thông tin điện tử của Ủy ban nhân dân huyện X:

Căn cứ phạm vi, quy mô và đối tượng phục vụ của hệ thống, Trang thông tin điện tử của Ủy ban nhân dân huyện X chỉ cung cấp thông tin trên mạng Internet về chức năng, quyền hạn, nhiệm vụ, tổ chức bộ máy và các thông tin khác phục vụ cho hoạt động của Ủy ban nhân dân huyện và các cơ quan chuyên môn, đơn vị trực thuộc Ủy ban nhân dân huyện; người sử dụng không cần tài khoản đăng nhập đều có thể đọc và khai thác thông tin. Do đó, theo quy định tại điểm a Khoản 2 và điểm a Khoản 1 Điều 6 Nghị định số 85/2016/NĐ-CP, Trang thông tin điện tử của Ủy ban nhân dân huyện X là hệ thống thông tin phục vụ hoạt động nội bộ, chỉ xử lý thông tin công cộng.

Vì vậy, căn cứ quy định tại Điều 7 Nghị định số 85/2016/NĐ-CP, đề xuất Trang thông tin điện tử của Ủy ban nhân dân huyện X là hệ thống thông tin cấp độ 1.

4.3. Thuyết minh bổ sung đối với các hệ thống thông tin được được đề xuất cấp độ 4 hoặc cấp độ 5

Căn cứ quy định tại khoản 5 Điều 8 Thông tư số 12/2022/TT-BTTTT, đối với các hệ thống thông tin được được đề xuất cấp độ 4 hoặc cấp độ 5, ngoài các nội dung phải thuyết minh tại các Mục 4.1 và 4.2 ở trên, cần bổ sung, làm rõ:

(1) 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;

(2) 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;

(3) 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;

(4) 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 Nghị định số 85/2016/NĐ-CP.

5. Thuyết minh phương án bảo đảm an toàn thông tin

Căn cứ quy định tại khoản 6 Điều 8 Thông tư số 12/2022/TT-BTTTT, thuyết minh phương án bảo đảm an toàn thông tin bao gồm các nội dung:

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

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

Nội dung thuyết minh phương án bảo đảm an toàn thông tin phải đảm bảo tuân thủ các quy định tại Điều 19 Nghị định số 85/2016/NĐ-CP; Điều 9, Điều 10 và Phụ lục tương ứng với cấp độ đề xuất được ban hành kèm theo Thông tư số 12/2022/TT-BTTTT. Đặc biệt, căn cứ các quy định tại khoản 1 và khoản 2 Điều 9 Thông tư số 12/2022/TT-BTTTT:

- Việc bảo đảm an toàn hệ thống thông tin theo cấp độ thực hiện theo yêu cầu cơ bản quy định tại Thông tư 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;

- Yêu cầu cơ bản đối với từng cấp độ quy định tại Thông tư ***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 (yêu cầu an toàn vật lý áp dụng đối với công trình xây dựng phòng máy chủ, trung tâm dữ liệu, điện toán đám mây phục vụ vận hành hệ thống thông tin). Do đó, trong thực tiễn, tùy thuộc vào đánh giá về mức độ quan trọng của từng hệ thống thông tin cụ thể, đơn vị vận hành hệ thống thông tin hoàn toàn ***có thể đề xuất triển khai bổ sung*** một hoặc một số biện pháp bảo vệ (về quản lý và kỹ thuật) ở cấp độ cao hơn để tăng cường bảo vệ cho hệ thống thông tin.

5.1. Thuyết minh phương án đáp ứng các yêu cầu về quản lý tương ứng với cấp độ đề xuất

5.1.1. Các yêu cầu cơ bản về quản lý đối với hệ thống thông tin

STT	Yêu cầu	Cấp độ				
		1	2	3	4	5
1	*Thiết lập chính sách an toàn thông tin*	x	x	x	x	x
1.1	Chính sách an toàn thông tin	x	x	x	x	x
1.2	Xây dựng và công bố	x	x	x	x	x
1.3	Rà soát, sửa đổi	x	x	x	x	x
2	*Tổ chức bảo đảm an toàn thông tin*	x	x	x	x	x
2.1	Đơn vị chuyên trách về an toàn thông tin	x	x	x	x	x
2.2	Phối hợp với cơ quan/tổ chức có thẩm quyền	x	x	x	x	x
3	*Bảo đảm nguồn nhân lực*	x	x	x	x	x
3.1	Tuyển dụng	x	x	x	x	x

3.2	Trong quá trình làm việc	x	x	x	x	x
3.3	Chấm dứt hoặc thay đổi công việc	x	x	x	x	x
4	*Quản lý thiết kế, xây dựng hệ thống*	x	x	x	x	x
4.1	Thiết kế an toàn hệ thống thông tin	x	x	x	x	x
4.2	Phát triển phần mềm thuê khoán		x	x	x	x
4.3	Thử nghiệm và nghiệm thu hệ thống	x	x	x	x	x
5	*Quản lý vận hành hệ thống*	x	x	x	x	x
5.1	Quản lý an toàn mạng	x	x	x	x	x
5.2	Quản lý an toàn máy chủ và ứng dụng	x	x	x	x	x
5.3	Quản lý an toàn dữ liệu	x	x	x	x	x
5.4	Quản lý an toàn thiết bị đầu cuối			x	x	x
5.5	Quản lý phòng chống phần mềm độc hại			x	x	x
5.6	Quản lý giám sát an toàn hệ thống thông tin			x	x	x
5.7	Quản lý điểm yếu an toàn thông tin			x	x	x
5.8	Quản lý sự cố an toàn thông tin		x	x	x	x
5.9	Quản lý an toàn người sử dụng đầu cuối		x	x	x	x
6	*Phương án quản lý rủi ro an toàn thông tin*	x	x	x	x	x
7	*Phương án kết thúc vận hành, khai thác, thanh lý, hủy bỏ*	x	x	x	x	x

Bảng 6. Tổng hợp các yêu cầu cơ bản về quản lý theo cấp độ tương ứng

Lưu ý:

(1) Đối với từng cấp độ an toàn thông tin, mỗi yêu cầu cơ bản về quản lý sẽ đặt ra một số tiêu chí an toàn cơ bản cần đáp ứng, chi tiết xem tại Tiêu chuẩn quốc gia TCVN 11930:2017;

(2) Trong quá trình thuyết minh phương án đáp ứng các yêu cầu về quản lý sẽ phải tham chiếu đến một số văn bản, chính sách có liên quan. Do đó, cần có danh mục tổng hợp các văn bản, chính sách có liên quan, được tham chiếu để thuận tiện trong việc theo dõi, rà soát, cập nhật cũng như thẩm định hồ sơ đề xuất cấp độ;

(3) Khi tham chiếu đến các văn bản, cần chỉ rõ nội dung, điểm, khoản, Điều tương ứng để làm rõ minh chứng.

Ví dụ 4.4. Danh sách văn bản tham chiếu:

- Quyết định số …/QĐ-… ngày …/…/… của [Chức vụ người có thẩm quyền tại cơ quan chủ quản hệ thống thông tin] ban hành quy chế bảo đảm an toàn thông tin mạng tại [Tên chủ quản hệ thống thông tin][39];

- Quyết định số …/QĐ-… ngày …/…/… của [Tên đơn vị vận hành][40] ban hành quy chế bảo đảm an toàn thông tin cho [Tên hệ thống thông tin];

- Quyết định số …/… ngày …/…/… của [Chức vụ người có thẩm quyền tại cơ quan chủ quản hệ thống thông tin] quy định chức năng nhiệm vụ quyền hạn và cơ cấu tổ chức của [Tên đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin];

- Quyết định số …/QĐ-… ngày …/…/… của [Chức vụ người có thẩm quyền tại đơn vị quản lý hạ tầng Trung tâm dữ liệu] ban hành quy chế khai thác sử dụng và bảo đảm an toàn thông tin cho Trung tâm dữ liệu của …;

- Tài liệu thiết kế hệ thống thông tin;

- Trường hợp hệ thống thông tin đang trong giai đoạn vận hành khai thác, thuyết minh bổ sung các tài liệu: Tài liệu hướng dẫn sử dụng hệ thống thông tin, Tài liệu thiết kế hệ thống thông tin do Nhà thầu/Nhà cung cấp dịch vụ xây dựng;

- Các quy trình (trong trường hợp đã được ban hành)[41], các tài liệu khác...

(3) Đối với các tiêu chí, yêu cầu về quản lý **cần có quy trình để áp dụng** theo quy định, nhưng chưa được ban hành kèm theo các văn bản được tham chiếu, hồ sơ đề xuất cấp độ cần đặt ra thời hạn hoàn thành việc xây dựng, ban hành các quy trình để đơn vị chủ trì xây dựng văn bản/quy chế có liên quan hoặc đơn vị được giao nhiệm vụ thống nhất thực hiện. Chẳng hạn: Trong vòng **03 tháng** kể từ ngày hệ thống thông tin được phê duyệt cấp độ an toàn thông tin.

5.1.2. Hướng dẫn thuyết minh thiết lập chính sách an toàn thông tin

Các yêu cầu thiết lập chính sách an toàn thông tin tập trung vào việc yêu cầu cấp có thẩm quyền ban hành văn bản thể hiện chính sách an toàn thông tin đảm bảo việc quản lý, vận hành hoạt động bình thường của hệ thống, trong đó:

(1) Chính sách an toàn thông tin: Thuyết minh thể hiện đã xây dựng quy chế bảo đảm an toàn thông tin cho hệ thống thông tin;

(2) Xây dựng và công bố: Thuyết minh thể hiện quy chế bảo đảm an toàn thông tin cho hệ thống thông tin đã được cấp có thẩm quyền ban hành;

(3) Rà soát, sửa đổi: Thuyết minh thể hiện định kỳ 03 năm (đối với cấp độ 1 và cấp độ 2) / 02 năm (đối với cấp độ 3) / hàng năm (đối với cấp độ 4) / 06 tháng (đối với cấp độ 5) rà soát các chính sách bảo đảm an toàn thông tin đối với hệ thống thông tin để điều chỉnh (nếu cần). Có thể đưa ra minh chứng quy chế

[39] Quy chế chung (nếu có).

[40] Trong trường hợp đơn vị vận hành hệ thống thông tin thuê dịch vụ hạ tầng của doanh nghiệp hoặc đặt hệ thống tại Trung tâm dữ liệu do một đơn vị khác quản lý, vận hành thì hai đơn vị có thể ký quy chế phối hợp.

[41] Ví dụ: Yêu cầu về quản lý tương ứng với cấp độ 1 có 2 quy trình cần ban hành gồm: Quy trình quản lý vận hành hoạt động bình thường của hạ tầng mạng và Quy trình quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ.

bảo đảm an toàn thông tin cho hệ thống thông tin đã được cập nhật, điều chỉnh, bổ sung hoặc thay thế (nếu có).

5.1.3. Hướng dẫn thuyết minh tổ chức bảo đảm an toàn thông tin

Các yêu cầu về tổ chức bảo đảm an toàn thông tin tập trung vào việc tổ chức bộ máy của đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin, trong đó:

(1) Đơn vị chuyên trách về an toàn thông tin: Thuyết minh tham chiếu đến các nhiệm vụ, quyền hạn của đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin đã được ban hành tại Quyết định quy định chức năng nhiệm vụ quyền hạn và cơ cấu tổ chức và quy chế chung về bảo đảm an toàn thông tin mạng do chủ quản hệ thống thông tin ban hành (nếu có).

(2) Phối hợp với cơ quan/tổ chức có thẩm quyền, các tiêu chí

- Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin: Cơ quan có thẩm quyền quản lý về an toàn thông tin là Bộ Thông tin và Truyền thông (Cục An toàn thông tin);

- Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin;

- Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền (từ cấp độ 2 trở lên),

Với các tiêu chí ở trên cần chỉ rõ bộ phận thuộc đơn vị chuyên trách về an toàn thông tin và bộ phận thuộc đơn vị vận hành hệ thống thông tin sẽ phối hợp, tham gia các hoạt động. Bổ sung quyết định quy định chức năng nhiệm vụ của bộ phận thuộc đơn vị chuyên trách về an toàn thông tin được giao nhiệm vụ để minh chứng (nếu có).

5.1.4. Hướng dẫn thuyết minh bảo đảm nguồn nhân lực

Các yêu cầu về bảo đảm nguồn nhân lực tập trung vào việc tuyển dụng các vị trí làm về an toàn thông tin phải đảm bảo chuyên môn đáp ứng yêu cầu, tổ chức các hoạt động nâng cao nhận thức về an toàn thông tin cho các cán bộ, người sử dụng thuộc phạm vi quản lý, trong đó:

(1) Tuyển dụng:

- Thuyết minh tham chiếu đến các quy định trong chính sách tuyển dụng hoặc đề án vị trí việc làm của đơn vị chuyên trách về an toàn thông tin đã được cấp có thẩm quyền ban hành;

- Đối với hệ thống thông tin từ cấp độ 3 trở lên cần có tham chiếu đến quy trình tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ;

(2) Trong quá trình làm việc: Có thể thuyết minh, tham chiếu đến các quy định được ban hành trong quy chế chung về bảo đảm an toàn thông tin mạng do chủ quản hệ thống thông tin ban hành hoặc quy chế riêng đối với hệ thống thông tin nếu có quy định riêng;

(3) Chấm dứt hoặc thay đổi công việc:

- Tương tự đối với các tiêu chí thuộc yêu cầu trong quá trình làm việc, có thể thuyết minh, tham chiếu đến các quy định được ban hành trong quy chế chung về bảo đảm an toàn thông tin mạng do chủ quản hệ thống thông tin ban hành hoặc quy chế riêng đối với hệ thống thông tin nếu có quy định riêng;

- Đối với hệ thống thông tin từ cấp độ 2 trở lên cần có quy trình và 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.

5.1.5. Hướng dẫn thuyết minh quản lý thiết kế, xây dựng hệ thống

Các yêu cầu về quản lý thiết kế, xây dựng hệ thống thông tin tập trung đặt ra các chính sách bảo đảm an toàn thông tin trong giai đoạn thiết kế, phát triển, thử nghiệm và nghiệm thu hệ thống, trong đó:

(1) Thiết kế an toàn hệ thống thông tin:

- Cần có đầy đủ các tài liệu môt tả thiết kế hệ thống; các tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ, phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin và khi có thay đổi thiết kế (từ cấp độ 2 trở lên): Cần có thuyết minh, tham chiếu đến các tài liệu đã được xây dựng;

- Cần đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống (từ cấp độ 2 trở lên): Báo cáo kinh tế - kỹ thuật, báo cáo nghiên cứu khả thi, kế hoạch thuê dịch vụ công nghệ thông tin, đề cương và dự toán chi tiết nâng cấp, mở rộng hệ thống thông tin cần có thuyết minh, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đã đặt ra;

- Có phương án quản lý và bảo vệ hồ sơ thiết kế (cấp độ 4, 5): Có thể thuyết minh, tham chiếu đến các quy định được ban hành trong quy chế chung về bảo đảm an toàn thông tin mạng do chủ quản hệ thống thông tin ban hành hoặc quy chế riêng đối với hệ thống thông tin nếu có quy định riêng;

- Có bộ phận chuyên môn, tổ chuyên gia đánh giá hồ sơ thiết kế hệ thống thông tin, các biện pháp bảo đảm an toàn thông tin trước khi triển khai thực hiện (cấp độ 4, 5): Cần có thuyết minh, tham chiếu đến các văn bản thành lập bộ phận chuyên môn, tổ chuyên gia phù hợp.

(2) Phát triển phần mềm thuê khoán (từ cấp độ 2 trở lên): Thuyết minh, tham chiếu đến nội dung thuyết minh tương ứng trong Báo cáo kinh tế - kỹ thuật, báo cáo nghiên cứu khả thi, kế hoạch thuê dịch vụ công nghệ thông tin, đề cương và dự toán chi tiết hoặc Hợp đồng đã ký với nhà phát triển. Lưu ý:

- Có yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm *(trừ trường hợp thuê dịch vụ công nghệ thông tin sẵn có trên thị trường)*;

- Từ cấp độ 3 trở lên cần tổ chức kiểm thử phần mềm trên môi trường thử nghiệm và kiểm tra, đánh giá an toàn thông tin trước khi đưa vào sử dụng.

Trường hợp hệ thống thông tin đang vận hành, cần tham chiếu đến các báo cáo, biên bản bàn giao, biên bản xác nhận kiểm thử, kiểm tra, đánh giá an toàn thông tin trước khi đưa vào sử dụng theo yêu cầu.

(3) Thử nghiệm và nghiệm thu hệ thống: Tương tự đối với phát triển phần mềm thuê khoán, cần có thuyết minh, tham chiếu đến nội dung thuyết minh tương ứng trong Báo cáo kinh tế - kỹ thuật, báo cáo nghiên cứu khả thi, kế hoạch thuê dịch vụ công nghệ thông tin, đề cương và dự toán chi tiết hoặc Hợp đồng đã ký với nhà phát triển. Trường hợp hệ thống thông tin đang vận hành, cần tham chiếu đến các báo cáo, biên bản bàn giao, biên bản xác nhận có liên quan.

Từ cấp độ 2 trở lên cần có quy trình thử nghiệm và nghiệm thu hệ thống (thường được chủ đầu tư và nhà phát triển thống nhất trong các phụ lục kèm theo của Hợp đồng đã ký).

5.1.6. Hướng dẫn thuyết minh quản lý vận hành hệ thống

Đây là phần chính của quy chế bảo đảm an toàn thông tin đối với hệ thống thông tin, trong đó cần có đầy đủ các quy định về bảo đảm an toàn đối với 4 thành phần của hệ thống thông tin gồm: Bảo đảm an toàn mạng, bảo đảm an toàn máy chủ, bảo đảm an toàn ứng dụng và bảo đảm an toàn dữ liệu.

Đối với các hệ thống thông tin từ cấp độ 2 trở lên cần có thêm quy định, quy trình bảo đảm an toàn người sử dụng đầu cuối, quản lý sự cố an toàn thông tin; đối với các hệ thống thông tin từ cấp độ 3 trở lên bổ sung thêm các quy định, quy trình quản lý an toàn thiết bị đầu cuối, quản lý phòng chống phần mềm độc hại, quản lý giám sát an toàn hệ thống thông tin và quản lý điểm yếu an toàn thông tin.

Trong quá trình thuyết minh, đối với các tiêu chí, yêu cầu được đặt ra trong Tiêu chuẩn quốc gia TCVN 11930:2017, tuy nhiên đơn vị vận hành hệ thống thông tin đề xuất không áp dụng thì cần làm thuyết minh, làm rõ lý do không áp dụng.

5.1.7. Hướng dẫn thuyết minh phương án quản lý rủi ro an toàn thông tin

Phương án quản lý rủi ro an toàn thông tin không được quy định trong Tiêu chuẩn quốc gia TCVN 11930:2017 nhưng được yêu cầu tại điểm d khoản 2 Điều 19 Nghị định số 85/2016/NĐ-CP và điểm e khoản 3 Điều 9 Thông tư số 12/2022/TT-BTTTT. Việc thuyết minh phương án quản lý rủi ro an toàn thông tin có thể tham chiếu đến các quy định được ban hành trong quy chế chung về bảo đảm an toàn thông tin mạng do chủ quản hệ thống thông tin ban hành hoặc quy chế riêng đối với hệ thống thông tin nếu có quy định riêng.

5.1.8. Hướng dẫn thuyết minh phương án kết thúc vận hành, khai thác, thanh lý, hủy bỏ

Tương tự phương án quản lý rủi ro an toàn thông tin, phương án kết thúc vận hành, khai thác, thanh lý, hủy bỏ không được quy định trong Tiêu chuẩn

quốc gia TCVN 11930:2017 nhưng được yêu cầu tại điểm g khoản 2 Điều 19 Nghị định số 85/2016/NĐ-CP và điểm g khoản 3 Điều 9 Thông tư số 12/2022/TT-BTTTT. Việc thuyết minh phương án kết thúc vận hành, khai thác, thanh lý, hủy bỏ có thể tham chiếu đến các quy định được ban hành trong quy chế chung về bảo đảm an toàn thông tin mạng do chủ quản hệ thống thông tin ban hành hoặc quy chế riêng đối với hệ thống thông tin nếu có quy định riêng.

Bên cạnh đó cần tham chiếu đến các nội dung tương ứng được thuyết minh trong kế hoạch thuê dịch vụ công nghệ thông tin và các điều khoản, phụ lục tương ứng trong Hợp đồng thuê dịch vụ trong trường hợp áp dụng hình thức thuê dịch vụ công nghệ thông tin.

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

5.2.1. Các yêu cầu cơ bản về kỹ thuật đối với hệ thống thông tin

STT	Yêu cầu	Cấp độ				
		1	**2**	**3**	**4**	**5**
1	*Bảo đảm an toàn mạng*	x	x	x	x	x
1.1	Thiết kế hệ thống	x	x	x	x	x
1.2	Kiểm soát truy cập từ bên ngoài mạng	x	x	x	x	x
1.3	Kiểm soát truy cập từ bên trong mạng		x	x	x	x
1.4	Nhật ký hệ thống	x	x	x	x	x
1.5	Phòng chống xâm nhập	x	x	x	x	x
1.6	Phòng chống phần mềm độc hại trên môi trường mạng			x	x	x
1.7	Bảo vệ thiết bị hệ thống	x	x	x	x	x
2	*Bảo đảm an toàn máy chủ*	x	x	x	x	x
2.1	Xác thực	x	x	x	x	x
2.2	Kiểm soát truy cập	x	x	x	x	x
2.3	Nhật ký hệ thống	x	x	x	x	x
2.4	Phòng chống xâm nhập	x	x	x	x	x
2.5	Phòng chống phần mềm độc hại	x	x	x	x	x
2.6	Xử lý máy chủ khi chuyển giao		x	x	x	x
3	*Bảo đảm an toàn ứng dụng*	x	x	x	x	x
3.1	Xác thực	x	x	x	x	x
3.2	Kiểm soát truy cập	x	x	x	x	x

3.3	Nhật ký hệ thống	x	x	x	x	x
3.4	Bảo mật thông tin liên lạc			x	x	x
3.5	Chống chối bỏ			x	x	x
3.6	An toàn ứng dụng và mã nguồn		x	x	x	x
4	*Bảo đảm an toàn dữ liệu*	x	x	x	x	x
4.1	Nguyên vẹn dữ liệu			x	x	x
4.2	Bảo mật dữ liệu		x	x	x	x
4.3	Sao lưu dự phòng	x	x	x	x	x

Bảng 7. Tổng hợp các yêu cầu cơ bản về kỹ thuật theo cấp độ tương ứng

Lưu ý:

(1) Đối với từng cấp độ an toàn thông tin, mỗi yêu cầu cơ bản về kỹ thuật cũng đặt ra một số tiêu chí an toàn cơ bản cần đáp ứng, chi tiết xem tại Tiêu chuẩn quốc gia TCVN 11930:2017;

(2) Trong quá trình thuyết minh, làm rõ phương án kỹ thuật bảo đảm an toàn thông tin:

- Đối với các tiêu chí, yêu cầu được đặt ra trong Tiêu chuẩn quốc gia TCVN 11930:2017, tuy nhiên đơn vị vận hành hệ thống thông tin đề xuất không áp dụng thì cần làm thuyết minh, làm rõ lý do không áp dụng;

- Đối với các tiêu chí, yêu cầu được đặt ra có áp dụng nhưng chưa đáp ứng thì cần làm rõ phương án và kế hoạch khắc phục (có thời hạn cụ thể) để đáp ứng yêu cầu, chẳng hạn.

Ví dụ 4.5. Trong yêu cầu bảo đảm an toàn mạng, đối với phương án thiết kế hệ thống thông tin có đặt ra yêu cầu *"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"*. Tuy nhiên, hiện trạng hệ thống thông tin, Firewall FW01 chưa có giải pháp này thì có thể thuyết minh:

- Firewall FW01 hiện chưa được tích hợp tính năng phòng chống xâm nhập. Để sử dụng tính năng này, cần mua bổ sung license và kích hoạt sử dụng;

- Lộ trình thực hiện: Trong 03 tháng kể từ khi hệ thống thông tin được phê duyệt cấp độ an toàn thông tin.

Sau khi được bổ sung, cần cập nhật lại phương án triển khai cho phù hợp.

5.2.2. Hướng dẫn thuyết minh bảo đảm an toàn mạng

Phần này liên quan mật thiết đến thuyết minh mô hình kiến trúc, mô hình lô-gic, mô hình vật lý, các thiết bị mạng, thiết bị và giải pháp bảo đảm an toàn thông tin đã được mô tả trong các nội dung thuyết minh tổng quan về hệ thống thông tin, trong đó:

(1) Các yêu cầu về thiết kế hệ thống, kiểm soát truy cập từ bên ngoài mạng, kiểm soát truy cập từ bên trong mạng (từ cấp độ 2) và phòng chống phần mềm độc hại trên môi trường mạng (từ cấp độ 3): Thuyết minh đảm bảo đồng bộ với mô hình lô-gic, mô hình vật lý các thiết bị mạng, thiết bị và giải pháp bảo đảm an toàn thông tin đã được mô tả trong các nội dung thuyết minh tổng quan về hệ thống thông tin. Đối với các thiết bị mạng, thiết bị và giải pháp bảo đảm an toàn thông tin cần được đầu tư, mua sắm bổ sung thì cần làm rõ phương án và kế hoạch khắc phục (có thời hạn cụ thể) để đáp ứng yêu cầu;

(2) Các yêu cầu về nhật ký hệ thống, bảo vệ thiết bị hệ thống: Lập bảng thuyết minh đáp ứng các yêu cầu đối với các tiêu chí được đặt ra đối với các thiết bị mạng và thiết bị an toàn thông tin, trong đó:

- Dấu "+" thể hiện tiêu chí đã được thực hiện trên thiết bị (trường hợp thiết bị đang được sử dụng và đã cấu hình) hoặc đã có phương án thực hiện (trường hợp thiết bị cần được đầu tư, mua sắm bổ sung);

- Dấu "-" thể hiện tiêu chỉ chưa thể thực hiện được trên thiết bị. Tuy nhiên, khi tích dấu "-" cần chỉ ra phương án xử lý để thành dấu "+" hoặc nêu rõ lý do không thực hiện được.

Ví dụ 4.6. Đối với hệ thống thông tin cấp độ 1 có mô hình lô-gic được minh họa tại **Ví dụ 4.1** (Hình 5), mô hình vật lý được minh họa tại **Ví dụ 4.2** (Hình 8) và có danh sách thiết bị như tại **Bảng 2 Chương 4** ở trên, các tiêu chí về nhật ký hệ thống và bảo vệ thiết bị hệ thống có thể được thuyết minh như sau:

(i) Thiết kế các vùng mạng trong hệ thống theo chức năng:

STT	Yêu cầu	Hiện trạng	Mô tả phương án triển khai/Lý do không triển khai
1	Vùng mạng nội bộ	[Hiện trạng][42] Ví dụ: Đã có	[Mô tả phương án đã hoặc sẽ triển khai để đáp ứng hoặc Lý do không triển khai vùng mạng nội bộ] Ví dụ: Được thiết lập để cung cấp kết nối mạng cho các máy trạm và các thiết bị đầu cuối và các thiết bị khác của người sử dụng vào hệ thống.
2	Vùng mạng biên	[Hiện trạng] Ví dụ: Đã có	[Mô tả phương án đã hoặc sẽ triển khai để đáp ứng hoặc Lý do không triển khai vùng mạng biên] Ví dụ: Được thiết lập để cung cấp các kết nối hệ thống ra bên ngoài Internet và các mạng khác.

[42] Hiện trạng là một trong các trạng thái: **Đã có, Chưa có hoặc Không áp dụng.**

3	Vùng DMZ	[Hiện trạng] Ví dụ: Đã có	[Mô tả phương án đã hoặc sẽ triển khai để đáp ứng hoặc Lý do không triển khai vùng DMZ] Ví dụ: Được thiết lập để đặt các máy chủ công cộng, cho phép truy cập trực tiếp từ các mạng bên ngoài và mạng Internet.

(ii) Các yêu cầu đối với phương án thiết kế:

STT	Yêu cầu	Hiện trạng	Mô tả phương án triển khai/Lý do không triển khai
1	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	[Hiện trạng] Ví dụ: Đã có	[Mô tả phương án đã hoặc sẽ triển khai để đáp ứng hoặc Lý do không triển khai yêu cầu này] Ví dụ: Firewall FW01 đã được tích hợp tính năng quản lý truy cập từ xa VPN. Trường hợp hệ thống có sự cố cần xử lý từ xa, quản trị hệ thống sẽ sử dụng tài khoản VPN kết nối, đăng nhập và truy cập vào các máy chủ được đặt tại vùng DMZ để xử lý.
2	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	[Hiện trạng] Ví dụ: Chưa có	[Mô tả phương án đã hoặc sẽ triển khai để đáp ứng hoặc Lý do không triển khai yêu cầu này] Ví dụ: Firewall FW01 hiện chưa được tích hợp tính năng phòng chống xâm nhập. Để sử dụng tính năng này, cần mua bổ sung license và kích hoạt sử dụng. Lộ trình thực hiện: Trong **03 tháng** kể từ khi hệ thống thông tin được phê duyệt cấp độ an toàn thông tin[43].
3	Có phương án phòng chống mã độc cho máy chủ và máy trạm sử dụng sản phẩm	[Hiện trạng] Ví dụ: Đã có	[Mô tả phương án đã hoặc sẽ triển khai để đáp ứng hoặc Lý do không triển khai yêu cầu này] Ví dụ: Các máy chủ và máy trạm tham gia vào hệ thống gồm DNS

[43] Lưu ý: Sau khi được bổ sung, cần cập nhật lại phương án triển khai cho phù hợp.

	Phòng chống mã độc hoặc phương án tương đương		Server, Server 01, PC 01 và PC 02 đều đã được cài đặt phần mềm diệt virus McAfee có bản quyền. Đối với máy chủ Server 02, sau khi được mua sắm và được cài đặt để đưa vào sử dụng cũng sẽ được cài đặt phần mềm diệt virus McAfee có bản quyền.

(iii) Kiểm soát truy cập từ bên ngoài mạng:

STT	Yêu cầu	Hiện trạng	Mô tả phương án triển khai/Lý do không triển khai
1	Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập thông tin nội bộ hoặc quản trị hệ thống từ các mạng bên ngoài và mạng Internet	[Hiện trạng] Ví dụ: Đã có	[Mô tả phương án đã hoặc sẽ triển khai để đáp ứng hoặc Lý do không triển khai yêu cầu này] Ví dụ: Firewall FW01 được thiết lập chỉ cho phép truy cập đến các máy chủ tại vùng DMZ để quản trị thông qua VPN được tích hợp trên Firewall.
2	Kiểm soát truy cập từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể; chặn tất cả truy cập tới các dịch vụ, ứng dụng mà hệ thống không cung cấp hoặc không cho phép truy cập từ bên ngoài	[Hiện trạng] Ví dụ: Đã có	[Mô tả phương án đã hoặc sẽ triển khai để đáp ứng hoặc Lý do không triển khai yêu cầu này] Ví dụ: Cấu hình Firewall FW01 từ vùng mạng biên ngắt kết nối tới tất cả các cổng dịch vụ trên các máy chủ thuộc vùng DMZ, chỉ mở cổng 80 và cho phép truy cập qua VPN được tích hợp trên Firewall.

(iv) Nhật ký hệ thống:

STT	Yêu cầu[44] / Thiết bị[45]	Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên các thiết bị mạng chính
1	Firewall FW01	+

[44] Các tiêu chí cần thiết lập, cấu hình đáp ứng yêu cầu theo Tiêu chuẩn TCVN 11930:2017.
[45] Các thiết bị mạng chính được xác định ở Bảng 2.

2	[…]	+

(v) Phòng chống xâm nhập:

STT	Yêu cầu	Hiện trạng	Mô tả phương án triển khai/Lý do không triển khai
1	Có phương án phòng chống xâm nhập để bảo vệ vùng DMZ	[Hiện trạng] Ví dụ: Chưa có	[Mô tả phương án đã hoặc sẽ triển khai để đáp ứng hoặc Lý do không triển khai yêu cầu này] Ví dụ: Cần mua bổ sung license cho Firewall FW01 và kích hoạt sử dụng tính năng phòng chống xâm nhập để bảo vệ vùng DMZ[46].
2	Định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng (Signatures)	[Hiện trạng] Ví dụ: Chưa có	[Mô tả phương án đã hoặc sẽ triển khai để đáp ứng hoặc Lý do không triển khai yêu cầu này] Ví dụ: Cần mua bổ sung license cho Firewall FW01 và kích hoạt sử dụng tính năng phòng chống xâm nhập[47].

(vi) Bảo vệ thiết bị hệ thống:

STT	Yêu cầu / Thiết bị[48]	a) Cấu hình chức năng xác thực trên các thiết bị hệ thống (nếu hỗ trợ) để xác thực người dùng khi quản trị thiết bị trực tiếp hoặc từ xa	b) Thiết lập cấu hình chỉ cho phép sử dụng các kết nối mạng an toàn (nếu hỗ trợ) khi truy cập, quản trị thiết bị từ xa
1	Router 01	+	+
2	Firewall FW01	+	+
3	Switch SW 01	+	+
4	Switch SW 02	+	+
5	Router 02	+	+
6	PC 01	+	+
7	PC 02	+	+
8	[…]	+	+

[46] Lưu ý: Sau khi được bổ sung, cần cập nhật lại phương án triển khai cho phù hợp.
[47] Lưu ý: Sau khi được bổ sung, cần cập nhật lại phương án triển khai cho phù hợp.
[48] Tất cả các thiết bị được nêu trong Bảng 2.

5.2.3. Hướng dẫn thuyết minh bảo đảm an toàn máy chủ

Tương tự đối với các tiêu chí về nhật ký hệ thống và bảo vệ thiết bị hệ thống tại **Mục 5.2.2** ở trên, việc thuyết minh bảo đảm an toàn máy chủ cũng áp dụng hình thức lập bảng thuyết minh. Phần này *áp dụng đối với tất cả các máy chủ* được sử dụng để cài đặt, vận hành hệ thống thông tin.

Ví dụ 4.7. Đối với hệ thống thông tin cấp độ 1 có mô hình lô-gic được minh họa tại **Ví dụ 4.1** (Hình 5), mô hình vật lý được minh họa tại **Ví dụ 4.2** (Hình 8) và có danh sách máy chủ như tại **Bảng 3 Chương 4** ở trên:

(i) Xác thực:

STT	**Yêu cầu** / **Máy chủ**[49]	**a) Thiết lập chính sách xác thực trên máy chủ để xác thực người dùng khi truy cập, quản lý và sử dụng máy chủ**	**b) Thay đổi các tài khoản mặc định trên hệ thống hoặc vô hiệu hóa (nếu không sử dụng)**	**c) Thiết lập cấu hình máy chủ để đảm bảo an toàn mật khẩu người sử dụng, bao gồm các yêu cầu sau: - Yêu cầu thay đổi mật khẩu mặc định; - Thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự**
1	DNS Server	+[50]	+	+
2	Server 01	+	+	+
3	Server 02	+	+	+
4	[…]	+	+	+

(ii) Kiểm soát truy cập:

STT	**Yêu cầu** / **Máy chủ**[51]	**Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa**
1	DNS Server	+
2	Server 01	+
3	Server 02	+
4	[…]	+

[49] Các máy chủ đã được xác định ở Bảng 3.

[50] Dấu "+" thể hiện tiêu chí đã được thực hiện trên máy chủ (trường hợp máy chủ đang được sử dụng và đã cấu hình) hoặc đã có phương án thực hiện (trường hợp máy chủ cần được đầu tư, mua sắm bổ sung). Dấu "-" thể hiện tiêu chí chưa thể thực hiện được trên máy chủ. Tuy nhiên, khi tích dấu "-" cần chỉ ra phương án xử lý để thành dấu "+" hoặc nêu rõ lý do không thực hiện được.

[51] Các máy chủ đã được xác định ở Bảng 3.

(iii) Nhật ký hệ thống:

STT	Yêu cầu / Máy chủ[52]	a) Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau: - Thông tin kết nối mạng tới máy chủ (Firewall log); - Thông tin đăng nhập vào máy chủ	b) Đồng bộ thời gian giữa máy chủ với máy chủ thời gian
1	DNS Server	+	+
2	Server 01	+	+
3	Server 02	+	+
4	[…]	+	+

(iv) Phòng chống xâm nhập:

STT	Yêu cầu / Máy chủ[53]	a) Loại bỏ các tài khoản không sử dụng, các tài khoản không còn hợp lệ trên máy chủ	b) Sử dụng tường lửa của hệ điều hành và hệ thống để cấm các truy cập trái phép tới máy chủ
1	DNS Server	+	+
2	Server 01	+	+
3	Server 02	+	+
4	[…]	+	+

(v) Phòng chống phần mềm độc hại:

STT	Yêu cầu / Máy chủ[54]	Cài đặt phần mềm phòng chống mã độc (hoặc có phương án khác tương đương) và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm
1	DNS Server	+
2	Server 01	+
3	Server 02	+
4	[…]	+

Lưu ý: Đối với hệ thống thông tin cấp độ 2 trở lên có thêm các tiêu chí về xử lý máy chủ khi chuyển giao.

[52] Các máy chủ đã được xác định ở Bảng 3.
[53] Các máy chủ đã được xác định ở Bảng 3.
[54] Các máy chủ đã được xác định ở Bảng 3.

5.2.4. Hướng dẫn thuyết minh bảo đảm ứng dụng

Tương tự đối với việc thuyết minh bảo đảm an toàn máy chủ, thuyết minh bảo đảm an toàn ứng dụng cũng áp dụng hình thức lập bảng thuyết minh. Phần này áp dụng đối với tất cả các ứng dụng phần mềm của hệ thống thông tin.

Ví dụ 4.8. Đối với hệ thống thông tin cấp độ 1 có mô hình lô-gic được minh họa tại **Ví dụ 4.1** (Hình 5), mô hình vật lý được minh họa tại **Ví dụ 4.2** (Hình 8) và có danh sách ứng dụng như tại **Bảng 3 Chương 4** ở trên:

(i) Xác thực:

STT	**Yêu cầu** / **Ứng dụng**[55]	**a) Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng**	**b) Lưu trữ có mã hóa thông tin xác thực hệ thống**	**c) Thiết lập cấu hình ứng dụng để đảm bảo an toàn mật khẩu người sử dụng, bao gồm các yêu cầu sau: - Yêu cầu thay đổi mật khẩu mặc định; - Thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự**
1	[Tên ứng dụng / dịch vụ 1. Ví dụ: Trang thông tin điện tử của Ủy ban nhân dân huyện X]	+[56]	+	+
2	[…]	+	+	+

(ii) Kiểm soát truy cập:

STT	**Yêu cầu** / **Ứng dụng**[57]	**a) Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị ứng dụng từ xa**	**b) Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng**
1	[Tên ứng dụng/dịch vụ 1. Ví dụ: Trang thông tin điện tử của Ủy ban nhân	+	+

[55] Các ứng dụng, dịch vụ đã được xác định ở Bảng 3.

[56] Dấu "+" thể hiện tiêu chí đã được thực hiện trên ứng dụng/dịch vụ (trường hợp ứng dụng/dịch vụ đang sử dụng và đã cấu hình) hoặc đã có phương án thực hiện (trường hợp ứng dụng/dịch vụ chưa đưa vào sử dụng). Dấu "-" thể hiện tiêu chí chưa thể thực hiện được trên ứng dụng. Tuy nhiên, khi tích dấu "-" cần chỉ ra phương án xử lý để thành dấu "+" hoặc nêu rõ lý do không thực hiện được.

[57] Các ứng dụng, dịch vụ đã được xác định ở Bảng 3.

	dân huyện X]		
2	[…]	+	+

(iii) Nhật ký hệ thống:

STT	Yêu cầu / Ứng dụng[58]	Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau: - Thông tin truy cập ứng dụng; - Thông tin đăng nhập khi quản trị ứng dụng
1	[Tên ứng dụng/dịch vụ 1. Ví dụ: Trang thông tin điện tử của Ủy ban nhân dân huyện X]	+
2	[…]	+

Lưu ý: Đối với hệ thống thông tin cấp độ 2 trở lên có thêm các tiêu chí về an toàn ứng dụng và mã nguồn; cấp độ 3 trở lên có thểm các tiêu chí về bảo mật thông tin liên lạc và chống chối bỏ.

5.2.5. Hướng dẫn thuyết minh bảo đảm an toàn dữ liệu

Lập bảng thuyết minh đáp ứng:

Ví dụ 4.9. Tiếp tục lấy ví dụ minh họa đối với hệ thống thông tin cấp độ 1 có mô hình lô-gic được minh họa tại **Ví dụ 4.1** (Hình 5), mô hình vật lý được minh họa tại **Ví dụ 4.2** (Hình 8) và có danh sách ứng dụng như tại **Bảng 3 Chương 4** ở trên:

(i) Sao lưu dự phòng:

STT	Yêu cầu	Hiện trạng	Mô tả phương án triển khai/Lý do không triển khai
1	Thực hiện sao lưu dự phòng các thông tin, dữ liệu quan trọng trên hệ thống	[Hiện trạng] Ví dụ: Chưa có	[Mô tả phương án đã hoặc sẽ triển khai để đáp ứng hoặc Lý do không triển khai yêu cầu này] Ví dụ: Bố trí máy chủ Server 02 để thực hiện sao lưu dữ liệu hàng ngày (cấu hình sao lưu vào nửa đêm). Định kỳ hàng tuần hoặc hàng tháng tiến hành xóa bớt các file sao lưu, chỉ để lại dữ liệu sao lưu của 07 ngày gần nhất[59].

[58] Các ứng dụng, dịch vụ đã được xác định ở Bảng 3.
[59] Lưu ý: Sau khi được bổ sung, cần cập nhật lại phương án triển khai cho phù hợp.

Lưu ý: Đối với hệ thống thông tin cấp độ 2 trở lên có thêm các tiêu chí về bảo mật dữ liệu; cấp độ 3 trở lên có thêm các tiêu chí về nguyên vẹn dữ liệu.

6. Quy chế bảo đảm an toàn thông tin cho hệ thống thông tin

6.1. Nguyên tắc xây dựng

Quy chế bảo đảm an toàn thông tin cho hệ thống thông tin là văn bản quy định các chính sách để *đảm bảo thực thi các phương án bảo đảm an toàn thông tin trong quá trình vận hành, kết thúc vận hành, khai thác, thanh lý, hủy bỏ*, tuân thủ quy định tại khoản 2 Điều 19 Nghị định số 85/2016/NĐ-CP, Thông tư số 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017.

Theo quy định tại khoản 7 Điều 9 Thông tư số 12/2022/TT-BTTTT, quy chế bảo đảm an toàn thông tin cho hệ thống phải được xây dựng, đáp ứng các yêu cầu an toàn về quản lý theo cấp độ an toàn 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. Quy định này nhằm đảm bảo các biện pháp bảo đảm an toàn thông tin về quản lý được thuyết minh trong hồ sơ đề xuất cấp độ có thể được áp dụng ngay khi hệ thống thông tin được phê duyệt cấp độ an toàn thông tin.

Lưu ý:

(1) Trường hợp chủ quản hệ thống thông tin hoặc đơn vị vận hành hệ thống thông tin *đã ban hành* quy chế bảo đảm an toàn thông tin chung hoặc quy chế chung trong việc quản lý, sử dụng, vận hành các hệ thống thông tin đã phù hợp với các tiêu chí bảo đảm an toàn thông tin về quản lý ứng với cấp độ được đề xuất của hệ thống thông tin được xây dựng hồ sơ đề xuất cấp độ thì có thể tham chiếu, áp dụng quy chế chung đó mà không cần xây dựng quy chế riêng;

(2) Trường hợp quy chế chung không đáp ứng yêu cầu: Cần xây dựng, bổ sung các chính sách theo phương án: (i) ban hành quy chế chung sửa đổi hoặc (ii) ban hành quy chế chung mới thay thế quy chế chung hiện tại hoặc (iii) ban hành các quy chế riêng theo nhóm các hệ thống thông tin có liên quan;

(3) Trong quá trình xây dựng, thẩm định hồ sơ đề xuất cấp độ, các biện pháp bảo đảm an toàn thông tin về quản lý *có thể tham chiếu đến các nội dung của quy chế đang trong giai đoạn xây dựng dự thảo*. Tuy nhiên, *khi phê duyệt hồ sơ đề xuất cấp độ thì phải dẫn chiếu đến nội dung của quy chế chính thức, **đã được ban hành***.

6.2. Cấp có thẩm quyền ban hành quy chế bảo đảm an toàn thông tin cho hệ thống thông tin

Bên cạnh việc áp dụng các văn bản hoặc quy chế chung về bảo đảm an toàn thông tin mạng do chủ quản hệ thống thông tin ban hành, trong trường hợp cần thiết phải ban hành quy chế bảo đảm an toàn thông tin riêng đối với hệ thống thông tin thì việc xác định cấp có thẩm quyền ban hành sẽ phụ thuộc vào phạm vi, quy mô, đối tượng áp dụng và cách thức triển khai của hệ thống thông tin đó, cụ thể:

(1) Trường hợp hệ thống thông tin được triển khai hoàn toàn chỉ trong phạm vi nội bộ của đơn vị vận hành hệ thống thông tin: Đơn vị vận hành hệ thống thông tin có thể tự xây dựng, ban hành quy chế;

(2) Trường hợp hệ thống thông tin được triển khai trong phạm vi nội bộ của đơn vị vận hành nhưng hệ thống được cài đặt, vận hành tại hạ tầng Trung tâm dữ liệu/Điện toán đám mây do đơn vị khác vận hành, khi đó đơn vị vận hành hệ thống thông tin và đơn vị vận hành hạ tầng kỹ thuật có thể phối hợp:

- Xây dựng, ban hành quy chế phối hợp bảo đảm an toàn thông tin, hoặc;

- Đồng trình chủ quản hệ thống thông tin ban hành nếu cả hai đơn vị cùng là đơn vị thuộc quyền quản lý của chủ quản hệ thống thông tin;

(3) Trường hợp hệ thống thông tin được triển khai dùng chung cho nhiều đơn vị, trong đó các đơn vị tham gia sử dụng hệ thống không thuộc phạm vi quản lý của đơn vị vận hành hệ thống thông tin: Đơn vị vận hành hệ thống thông tin tham mưu, trình chủ quản hệ thống thông tin ban hành quy chế.

6.3. Các quy trình liên quan

Ứng với quy chế bảo đảm an toàn thông tin **sẽ có các quy trình**.

Các quy trình có thể ban hành sau khi hồ sơ đề xuất cấp độ được phê duyệt, tuy nhiên hồ sơ đề xuất cấp độ phải chỉ rõ thời hạn hoàn thành các yêu cầu về quản lý mà chưa đáp ứng (chưa ban hành quy trình).

Tùy vào phạm vi đối tượng áp dụng của từng yêu cầu, các quy trình cụ thể có thể do chủ quản hệ thống thông tin, đơn vị chuyên trách về an toàn thông tin, đơn vị vận hành hệ thống thông tin, đơn vị quản lý, vận hành hạ tầng kỹ thuật hoặc các đơn vị khác được chủ quản hệ thống thông tin giao nhiệm vụ ban hành.

Ví dụ 4.10. Đối với các yêu cầu về quản lý của từng cấp độ an toàn hệ thống thông tin theo Tiêu chuẩn quốc gia TCVN 11930:2017:

(i) Hệ thống thông tin cấp độ 1: Có **02 yêu cầu** phải ban hành quy trình, do đó, tương ứng tối thiểu phải có 02 quy trình được ban hành, gồm:

- Quy trình quản lý, vận hành hoạt động bình thường của hạ tầng mạng;

- Quy trình quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ.

(ii) Hệ thống thông tin cấp độ 2: Có **07 yêu cầu** phải ban hành quy trình, do đó, tương ứng tối thiểu phải có 07 quy trình được ban hành, gồm:

- Quy trình và 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;

- Quy trình thử nghiệm và nghiệm thu hệ thống;

- Quy trình quản lý an toàn mạng;

- Quy trình quản lý an toàn máy chủ và ứng dụng;

- Quy trình quản lý an toàn dữ liệu;

- Quy trình quản lý sự cố an toàn thông tin;

- Quy trình quản lý an toàn người sử dụng đầu cuối.

(iii) Hệ thống thông tin cấp độ 3, 4, 5: Có **12 yêu cầu** phải ban hành quy trình, do đó, tương ứng tối thiểu phải có 12 quy trình được ban hành, gồm:

- Quy trình tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ (có thể do đơn vị phụ trách tổ chức cán bộ của chủ quản hệ thống tham mưu ban hành);
- Quy trình và 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;
- Quy trình thử nghiệm và nghiệm thu hệ thống;
- Quy trình quản lý an toàn mạng;
- Quy trình quản lý an toàn máy chủ và ứng dụng;
- Quy trình quản lý an toàn dữ liệu;
- Quy trình quản lý an toàn thiết bị đầu cuối;
- Quy trình quản lý phần mềm độc hại;
- Quy trình quản lý giám sát an toàn hệ thống thông tin;
- Quy trình quản lý điểm yếu an toàn thông tin;
- Quy trình quản lý sự cố an toàn thông tin;
- Quy trình quản lý an toàn người sử dụng đầu cuối.

TỔNG KẾT CHƯƠNG 4

1. Trong giai đoạn chuẩn bị đầu tư hoặc giai đoạn đầu tư: Hồ sơ đề xuất cấp độ an toàn thông tin cần được xây dựng song song và đồng bộ với nội dung thuyết minh phương án kỹ thuật trong tài liệu thiết kế hệ thống thông tin.

2. Nội dung hồ sơ đề xuất cấp độ:

- ❖ Phương án bảo đảm an toàn thông tin về quản lý phải được tham chiếu đến các văn bản, quy chế có liên quan, đã được ban hành khi trình phê duyệt cấp độ an toàn thông tin;
- ❖ Phương án bảo đảm an toàn thông tin về kỹ thuật nếu chưa đáp ứng thì phải đưa ra phương án và kế hoạch (có thời hạn) cụ thể khắc phục. Đây là căn cứ để tiến hành đầu tư, mua sắm bổ sung các thiết bị, giải pháp tương ứng để đảm bảo việc vận hành hệ thống được an toàn, đáp ứng yêu cầu của cấp độ tương ứng được đề xuất;
- ❖ Đối với các tiêu chí, yêu cầu (về quản lý và kỹ thuật) được đặt ra trong Tiêu chuẩn quốc gia TCVN 11930:2017 *nhưng đề xuất không áp dụng thì cần thuyết minh, làm rõ lý do không áp dụng*.

3. Tùy thuộc vào đánh giá về mức độ quan trọng của từng hệ thống thông tin cụ thể, đơn vị vận hành hệ thống thông tin hoàn toàn ***có thể đề xuất triển khai bổ sung*** một hoặc một số biện pháp bảo vệ (về quản lý và kỹ thuật) ở cấp độ cao hơn để tăng cường bảo vệ cho hệ thống thông tin.

Chương 5.
Thẩm định, phê duyệt cấp độ an toàn hệ thống thông tin

Sau khi đơn vị vận hành hệ thống thông tin hoàn thành việc xây dựng hồ sơ đề xuất cấp độ an toàn thông tin cho hệ thống thông tin, hồ sơ đề xuất cấp độ cần được cơ quan hoặc đơn vị có thẩm quyền tiến hành thẩm định và phê duyệt cấp độ an toàn thông tin để làm căn cứ triển khai các biện pháp bảo vệ tương ứng theo hồ sơ đề xuất cấp độ được phê duyệt.

Chương này sẽ hướng dẫn chi tiết các nội dung có liên quan đến quy trình thẩm định và phê duyệt cấp độ an toàn hệ thống thông tin. Đặc biệt, sẽ thống nhất hướng dẫn đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin cụ thể các nội dung chính, cần thuyết minh, làm rõ khi tiến hành thẩm định hồ sơ đề xuất cấp độ.

1. Thẩm quyền thẩm định, phê duyệt cấp độ

Thẩm quyền thẩm định và phê duyệt cấp độ an toàn thông tin đối với các hệ thống thông tin được quy định tại Điều 12 Nghị định số 85/2016/NĐ-CP như sau:

1.1. Đối với hệ thống thông tin đề xuất cấp độ 1 hoặc cấp độ 2

Đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin thực hiện thẩm định, phê duyệt hồ sơ đề xuất cấp độ đối với hệ thống thông tin được đề xuất là cấp độ 1 hoặc cấp độ 2.

1.2. Đối với hệ thống thông tin đề xuất cấp độ 3

a) Thẩm định: Đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin thực hiện thẩm định hồ sơ đề xuất cấp độ.

b) Phê duyệt: Chủ quản hệ thống thông tin phê duyệt cấp độ an toàn thông tin trên cơ sở ý kiến thẩm định của đơn vị chuyên trách về an toàn thông tin.

1.3. Đối với hệ thống thông tin đề xuất cấp độ 4 hoặc cấp độ 5

a) Thẩm định:

- Bộ Thông tin và Truyền thông chủ trì, phối hợp với Bộ Quốc phòng, Bộ Công an và các bộ, ngành liên quan thực hiện thẩm định hồ sơ đề xuất cấp độ, trừ trường hợp hệ thống thông tin do Bộ Quốc phòng hoặc Bộ Công an quản lý;

- Bộ Quốc phòng chủ trì, phối hợp với Bộ Thông tin và Truyền thông và bộ, ngành liên quan thực hiện thẩm định hồ sơ đề xuất cấp độ đối với hệ thống thông tin do Bộ Quốc phòng quản lý;

- Bộ Công an chủ trì, phối hợp với Bộ Thông tin và Truyền thông và bộ, ngành liên quan thực hiện thẩm định hồ sơ đề xuất cấp độ đối với hệ thống thông tin do Bộ Công an quản lý.

b) Phê duyệt:

- Chủ quản hệ thống thông tin phê duyệt cấp độ an toàn thông tin đối với hệ thống thông tin đề xuất cấp độ 4; phê duyệt phương án bảo đảm an toàn thông tin đối với hệ thống thông tin đề xuất cấp độ 5;

- Thủ tướng Chính phủ phê duyệt danh mục hệ thống thông tin cấp độ 5 (danh mục hệ thống thông tin quan trọng quốc gia)[60].

2. Tổ chức thẩm định hồ sơ đề xuất cấp độ

2.1. Hồ sơ gửi thẩm định

Căn cứ quy định tại Điều 15 Nghị định số 85/2016/NĐ-CP và khoản 7 Điều 9 Thông tư số 12/2022/TT-BTTTT, hồ sơ đề xuất cấp độ gửi thẩm định gồm các tài liệu sau đây:

(1) Văn bản đề nghị thẩm định, phê duyệt hồ sơ đề xuất cấp độ theo Mẫu số 01 được ban hành kèm theo Nghị định số 85/2016/NĐ-CP (đối với hệ thống thông tin đề xuất cấp độ 1 hoặc cấp độ 2) hoặc Văn bản đề nghị thẩm định hồ sơ đề xuất cấp độ theo Mẫu số 02 được ban hành kèm theo Nghị định số 85/2016/NĐ-CP (đối với hệ thống thông tin đề xuất cấp độ 3 trở lên).

(2) Tài liệu hồ sơ đề xuất cấp độ bao gồm các tài liệu thành phần sau đây:

- Tài liệu mô tả, thuyết minh tổng quan về hệ thống thông tin, có đầy đủ các nội dung theo quy định tại khoản 3 Điều 8 Thông tư số 12/2022/TT-BTTTT;

- Tài liệu thuyết minh về việc đề xuất cấp độ, có đầy đủ các nội dung theo quy định tại khoản 4 Điều 8 Thông tư số 12/2022/TT-BTTTT. Trường hợp hệ thống thông tin được đề xuất cấp độ 4 hoặc cấp độ 5, cần làm rõ thêm các nội dung theo quy định tại khoản 5 Điều 8 Thông tư số 12/2022/TT-BTTTT;

- Tài liệu thuyết minh phương án bảo đảm an toàn thông tin theo cấp độ tương ứng, có đầy đủ các nội dung thuyết minh đáp ứng các yêu cầu về quản lý và kỹ thuật ứng với cấp độ đề xuất, theo quy định tại khoản 6 Điều 8, Điều 9 và Điều 10 Thông tư số 12/2022/TT-BTTTT.

(3) Tài liệu thiết kế hệ thống thông tin: Xem hướng dẫn tại Chương 4.

(4) Dự thảo quy chế hoặc quy chế bảo đảm an toàn thông tin đã được cấp có thẩm quyền ban hành và các văn bản, quy chế được tham chiếu, áp dụng.

(5) Văn bản ý kiến chuyên môn của đơn vị chuyên trách về an toàn thông tin đối với hệ thống thông tin được đề xuất cấp độ 4 hoặc cấp độ 5.

Lưu ý:

- Đối với hệ thống thông tin được đề xuất cấp độ 1, 2 hoặc 3: Đơn vị vận hành hệ thống thông tin gửi 01 bộ hồ sơ gồm các tài liệu (1), (2), (3) và (4) cho đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin để tổ chức thẩm định;

[60] Đến nay mới có 01 danh mục được ban hành kèm theo Quyết định số 632/QĐ-TTg.

- Đối với hệ thống thông tin được đề xuất cấp độ 4 hoặc 5: Chủ quản hệ thống thông tin gửi văn bản (1) kèm theo 04 bộ hồ sơ gồm các tài liệu (2), (3), (4) và (5) cho Bộ Thông tin và Truyền thông (hoặc Bộ Công an hoặc Bộ Quốc phòng theo quy định) để tổ chức thẩm định.

2.2. Hình thức thẩm định

Tổ chức họp (họp lấy ý kiến chuyên môn hoặc họp Hội đồng thẩm định) hoặc lấy ý kiến bằng văn bản hoặc áp dụng cả hai hình thức.

2.3. Thẩm định hồ sơ đề xuất cấp độ

Sau khi nhận được đầy đủ hồ sơ hợp lệ theo quy định, cơ quan/đơn vị có thẩm quyền thẩm định hồ sơ đề xuất cấp độ (sau đây gọi tắt là đơn vị thẩm định) tiến hành thẩm định hồ sơ với các nội dung cụ thể như sau:

2.3.1. Nội dung thẩm định hồ sơ đề xuất cấp độ

Theo quy định tại khoản 1 Điều 16 Nghị định số 85/2016/NĐ-CP, nội dung thẩm định hồ sơ đề xuất cấp độ bao gồm:

(1) Sự phù hợp về việc đề xuất cấp độ;

(2) Sự phù hợp của phương án bảo đảm an toàn hệ thống thông tin trong thiết kế sơ bộ, thiết kế thi công hoặc tài liệu có giá trị tương đương theo cấp độ tương ứng (tài liệu thiết kế hệ thống thông tin);

(3) Sự phù hợp của phương án bảo đảm an toàn hệ thống thông tin trong quá trình vận hành hệ thống theo cấp độ tương ứng.

2.3.2. Thẩm định sự phù hợp về việc đề xuất cấp độ

a) Nội dung cần xem xét để làm rõ sự phù hợp đối với cấp độ đề xuất:

- Mô tả phạm vi, quy mô của hệ thống thông tin thuộc tài liệu mô tả, thuyết minh tổng quan về hệ thống thông tin;

- Nội dung tài liệu thuyết minh về việc đề xuất cấp độ;

- Các nội dung có liên quan mô tả, làm rõ phạm vi, quy mô của hệ thống thông tin thuộc tài liệu thiết kế hệ thống thông tin.

b) Ý kiến thẩm định cần làm rõ:

- Sự phù hợp giữa loại thông tin mà hệ thống thông tin xử lý, được thuyết minh trong tài liệu thuyết minh về việc đề xuất cấp độ với quy định tại khoản 1 Điều 6 Nghị định số 85/2016/NĐ-CP; sự phù hợp, đồng bộ với loại thông tin có tính bí mật cao nhất mà hệ thống thông tin xử lý được thuyết minh trong tài liệu thiết kế hệ thống thông tin;

- Sự phù hợp giữa loại hình hệ thống thông tin được thuyết minh trong tài liệu thuyết minh về việc đề xuất cấp độ với các quy định tại khoản 2 Điều 6 Nghị định số 85/2016/NĐ-CP; sự phù hợp, đồng bộ với các nội dung có liên quan mô tả, làm rõ phạm vi, quy mô của hệ thống thông tin thuộc tài liệu thiết kế hệ thống thông tin;

- Sự phù hợp giữa cấp độ được đề xuất, được thuyết minh trong tài liệu thuyết minh về việc đề xuất cấp độ với các tiêu chí xác định cấp độ được quy định từ Điều 7 đến Điều 11 Nghị định số 85/2016/NĐ-CP; sự phù hợp, đồng bộ với nội dung mô tả phạm vi, quy mô của hệ thống thông tin thuộc tài liệu mô tả, thuyết minh tổng quan về hệ thống thông tin và các nội dung có liên quan mô tả, làm rõ phạm vi, quy mô của hệ thống thông tin thuộc tài liệu thiết kế hệ thống thông tin;

- Trong trường hợp hệ thống thông tin được đề xuất cấp độ 4 hoặc 5: Cho ý kiến thêm về sự phù hợp đối với các nội dung đặc thù được thuyết minh trong tài liệu thuyết minh về việc đề xuất cấp độ theo quy định tại khoản 5 Điều 8 Thông tư số 12/2022/TT-BTTTT, đồng bộ với các nội dung có liên quan mô tả, làm rõ phạm vi, quy mô của hệ thống thông tin thuộc tài liệu thiết kế hệ thống thông tin.

c) Kết quả đánh giá:

- Nội dung thẩm định đánh giá là "Đạt" nếu tất cả các nội dung được cho ý kiến thẩm định theo hướng dẫn tại điểm b ở trên được đánh giá là phù hợp;

- Nội dung thẩm định đánh giá là "Không đạt" nếu có ít nhất một trong các nội dung được cho ý kiến thẩm định theo hướng dẫn tại điểm b ở trên được đánh giá là không phù hợp.

2.3.3. Thẩm định sự phù hợp của phương án bảo đảm an toàn hệ thống thông tin trong tài liệu thiết kế hệ thống thông tin

a) Nội dung cần xem xét:

- Mô tả hiện trạng kiến trúc hệ thống (đối với hệ thống thông tin đang vận hành) hoặc kiến trúc hệ thống (đối với hệ thống thông tin được xây dựng mới hoặc nâng cấp, mở rộng) thuộc tài liệu mô tả, thuyết minh tổng quan hệ thống thông tin;

- Nội dung tài liệu thuyết minh phương án bảo đảm an toàn thông tin theo cấp độ tương ứng;

- Dự thảo quy chế bảo đảm an toàn thông tin cho hệ thống thông tin hoặc quy chế đã được cấp có thẩm quyền ban hành;

- Các nội dung có liên quan, mô tả, làm rõ mô hình kiến trúc tổng thể, mô hình lô-gic, mô hình vật lý của hệ thống, thuyết minh phương án bảo đảm an toàn thông tin (về quản lý và kỹ thuật) thuộc tài liệu thiết kế hệ thống thông tin.

b) Ý kiến thẩm định:

- Đối với nội dung phương án đáp ứng các yêu cầu về quản lý tương ứng với cấp độ đề xuất được thuyết minh trong tài liệu thuyết minh phương án bảo đảm an toàn thông tin:

+ Cho ý kiến tổng quan về sự phù hợp và đầy đủ giữa các nội dung được thuyết minh với các quy định tại Điều 9, Điều 10 và Phụ lục tương ứng với cấp độ đề xuất được ban hành kèm theo Thông tư số 12/2022/TT-BTTTT;

+ Cho ý kiến về sự phù hợp và đồng bộ giữa nội dung về quản lý thiết kế, xây dựng hệ thống được thuyết minh trong hồ sơ đề xuất cấp độ với các nội dung quy định, quy trình kèm theo dự thảo quy chế bảo đảm an toàn thông tin cho hệ thống thông tin hoặc quy chế đã được cấp có thẩm quyền ban hành;

+ Cho ý kiến về sự phù hợp, đồng bộ giữa nội dung thuyết minh về quản lý thiết kế, xây dựng hệ thống với các nội dung về chính sách quản lý trong tài liệu thiết kế hệ thống thông tin. Ví dụ: Chính sách về quyền sở hữu thông tin, dữ liệu hình thành trong quá trình thuê dịch vụ công nghệ thông tin với phương án quản lý rủi ro an toàn thông tin và phương án kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin theo quy định tại khoản 2 Điều 19 Nghị định số 85/2016/TT-BTTTT và khoản 3 Điều 9 Thông tư số 12/2022/TT-BTTTT.

- Đối với thuyết minh phương án đáp ứng các yêu cầu về kỹ thuật tương ứng với cấp độ đề xuất được thuyết minh trong tài liệu thuyết minh phương án bảo đảm an toàn thông tin:

+ Cho ý kiến về sự phù hợp giữa nội dung mô tả hiện trạng kiến trúc hệ thống hoặc mô tả kiến trúc hệ thống thuộc tài liệu mô tả, thuyết minh tổng quan về hệ thống thông tin với các quy định tại điểm d khoản 3 Điều 8, Điều 9, Điều 10 và Phụ lục tương ứng với cấp độ đề xuất được ban hành kèm theo Thông tư số 12/2022/TT-BTTTT; sự phù hợp, đồng bộ với các nội dung có liên quan, mô tả, làm rõ mô hình kiến trúc tổng thể, mô hình lô-gic, mô hình vật lý của hệ thống thuộc tài liệu thiết kế hệ thống thông tin;

+ Cho ý kiến về sự phù hợp, đầy đủ giữa nội dung thuyết minh phương án đáp ứng các yêu cầu về kỹ thuật với các quy định tương ứng tại Điều 9, Điều 10 và Phụ lục tương ứng với cấp độ đề xuất được ban hành kèm theo Thông tư số 12/2022/TT-BTTTT; sự phù hợp, đồng bộ với các nội dung thuyết minh về yêu cầu kỹ thuật đối với hệ thống thông tin tài liệu thiết kế hệ thống thông tin;

+ Tài liệu thiết kế hệ thống thông tin phải có thuyết minh, làm rõ các yêu cầu về phần mềm nội bộ được quy định tại khoản 8 Điều 9 Thông tư số 12/2022/TT-BTTTT, đồng bộ với nội dung thuyết minh phương án đáp ứng các yêu cầu về kỹ thuật trong tài liệu thuyết minh phương án bảo đảm an toàn thông tin;

+ Trường hợp hệ thống thông tin được đề xuất cấp độ 3, 4 hoặc 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 quy định tương ứng tại khoản 9 và khoản 10 Điều 9 Thông tư số 12/2022/TT-BTTTT, đồng bộ với nội dung thuyết minh phương án đáp ứng các yêu cầu về kỹ thuật trong tài liệu thuyết minh phương án bảo đảm an toàn thông tin.

c) Kết quả đánh giá:

- Nội dung thẩm định đánh giá là "Đạt" nếu tất cả các nội dung được cho ý kiến thẩm định theo hướng dẫn tại điểm b ở trên được đánh giá là phù hợp;

- Nội dung thẩm định đánh giá là "Không đạt" nếu có ít nhất một trong các nội dung được cho ý kiến thẩm định theo hướng dẫn tại điểm b ở trên được đánh giá là không phù hợp.

2.3.4. Thẩm định sự phù hợp của phương án bảo đảm an toàn hệ thống thông tin trong quá trình vận hành hệ thống theo cấp độ tương ứng

a) Nội dung cần xem xét:

- Nội dung tài liệu thuyết minh phương án bảo đảm an toàn thông tin theo cấp độ tương ứng;

- Dự thảo quy chế bảo đảm an toàn thông tin cho hệ thống thông tin hoặc quy chế đã được cấp có thẩm quyền ban hành;

- Các nội dung có liên quan, mô tả, làm rõ thuyết minh phương án bảo đảm an toàn thông tin (về quản lý và kỹ thuật) thuộc tài liệu thiết kế hệ thống thông tin.

b) Nội dung thẩm định:

- Đối với thuyết minh phương án đáp ứng các yêu cầu về quản lý tương ứng với cấp độ đề xuất được thuyết minh trong tài liệu thuyết minh phương án bảo đảm an toàn thông tin: Cho ý kiến về sự phù hợp của các nội dung về quản lý (ngoài các nội dung về quản lý thiết kế, xây dựng hệ thống), khi đưa hệ thống thông tin vào vận hành khai thác.

- Đối với thuyết minh phương án đáp ứng các yêu cầu về kỹ thuật tương ứng với cấp độ đề xuất được thuyết minh trong tài liệu thuyết minh phương án bảo đảm an toàn thông tin, trên cơ sở hiện trạng các phương án bảo đảm an toàn thông tin về mặt kỹ thuật đang được triển khai, cho ý kiến về sự phù hợp của lộ trình triển khai đầy đủ phương án đáp ứng các yêu cầu về kỹ thuật trong quá trình vận hành hệ thống thông tin, bao gồm:

+ Trường hợp hạ tầng kỹ thuật phục vụ triển khai hệ thống thông tin chưa được thiết kế theo các phân vùng mạng đáp ứng yêu cầu tại Phụ lục tương ứng với cấp độ đề xuất được ban hành kèm theo Thông tư số 12/2022/TT-BTTTT: Cho ý kiến về sự phù hợp của lộ trình thực hiện phân tách các vùng mạng đáp ứng yêu cầu và phương án (về quản lỹ và kỹ thuật) tạm thời triển khai áp dụng trong giai đoạn phân vùng mạng chưa được thiết kế đáp ứng yêu cầu;

+ Đối với các yêu cầu về kỹ thuật hiện tại chưa đáp ứng: Cho ý kiến về sự phù hợp của lộ trình dự kiến thực hiện phương án triển khai đáp ứng đầy đủ các yêu cầu về kĩ thuật và phương án (về quản lỹ và kỹ thuật) tạm thời triển khai áp dụng trong giai đoạn chưa triển khai đáp ứng đầy đủ các yêu cầu về kỹ thuật.

c) Kết quả đánh giá:

- Nội dung thẩm định đánh giá là "Đạt" nếu tất cả các nội dung được cho ý kiến thẩm định theo hướng dẫn tại điểm b ở trên được đánh giá là phù hợp;

- Nội dung thẩm định đánh giá là "Không đạt" nếu có ít nhất một trong các nội dung được cho ý kiến thẩm định theo hướng dẫn tại điểm b ở trên được đánh giá là không phù hợp;

- Đối với hệ thông thông tin đang vận hành: Trong trường hợp kết quả đánh giá là "Không đạt" và nhận thấy hệ thống thông tin chưa đáp ứng điều kiện để vận hành an toàn, đơn vị thẩm định có thể cho ý kiến nêu rõ các nguy cơ gây mất an toàn thông tin có thể xảy ra đối với hệ thống và yêu cầu đơn vị vận hành khẩn trương triển khai các biện pháp để bảo đảm an toàn thông tin trong quá trình vận hành hoặc báo cáo chủ quản hệ thống thông tin cho dừng hệ thống để triển khai các biện pháp bảo đảm an toàn thông tin.

2.3.5. Kết quả thẩm định hồ sơ đề xuất cấp độ

a) Hình thức phát hành:

Đơn vị thẩm định hồ sơ đề xuất cấp độ phát hành Văn bản ý kiến thẩm định theo Mẫu số 04 được ban hành kèm theo Nghị định số 85/2016/NĐ-CP, gửi đơn vị vận hành hệ thống thông tin.

b) Kết luận thẩm định:

- Hồ sơ đề xuất cấp độ của hệ thống thông tin được thuyết minh là phù hợp với cấp độ đề xuất và đủ điều kiện trình cấp có thẩm quyền phê duyệt cấp độ an toàn thông tin hoặc phê duyệt phương án bảo đảm an toàn thông tin nếu tất cả các nội dung thẩm định được đánh giá là "Đạt";

- Hồ sơ đề xuất cấp độ của hệ thống thông tin được thuyết minh là chưa phù hợp theo cấp độ đề xuất nếu trong ý kiến thẩm định có nội dung được đánh giá "Không đạt". Khi đó, đơn vị vận hành hệ thống thông tin cần thuyết minh bổ sung hoặc giải trình, làm rõ đối với các nội dung được đánh giá không đạt, gửi lại hồ sơ cho đơn vị thẩm định để tiếp tục tiến hành quy trình thẩm định theo quy định.

2.4. Hội đồng thẩm định độc lập

Đối với hệ thống thông tin được đề xuất cấp độ 1, 2 hoặc 3, trường hợp đơn vị chuyên trách an toàn thông tin đồng thời được chủ quản hệ thống thông tin giao là đơn vị vận hành hệ thống thông tin, căn cứ hướng dẫn tại Điều 6 Thông tư số 12/2022/TT-BTTTT, để tổ chức thẩm định hồ sơ đề xuất cấp độ, đơn vị chuyên trách về an toàn thông tin thực hiện theo 01 trong 02 phương án sau đây:

(1) Phương án 01: Trình chủ quản hệ thống thông tin giao một đơn vị trực thuộc có đủ năng lực chủ trì, tổ chức thẩm định;

(2) Phương án 02: 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.

Trường hợp thực hiện theo phương án 01, đơn vị được chủ quản hệ thống thông tin giao nhiệm vụ tổ chức thẩm định hồ sơ đề xuất cấp độ thực hiện nhiệm vụ như vai trò đơn vị chuyên trách về an toàn thông tin đối với hệ thống thông

tin được giao thẩm định. Phần này sẽ tập trung làm rõ một số nội dung có liên quan đến việc tổ chức thẩm định theo phương án 02 – tổ chức Hội đồng thẩm định độc lập.

2.4.1. Về nhân sự Chủ tịch Hội đồng thẩm định

Đơn vị chuyên trách về an toàn thông tin báo cáo chủ quản hệ thống thông tin giao 01 Lãnh đạo cấp phó của người đứng đầu cơ quan chủ quản hệ thống thông tin hoặc 01 Lãnh đạo đơn vị chuyên trách an toàn thông tin hoặc 01 chuyên gia có uy tín trong lĩnh vực an toàn thông tin làm Chủ tịch Hội đồng thẩm định.

Ví dụ 5.1. Một số trường hợp điển hình:

(i) Đối với Hội đồng thẩm định độc lập do bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ hoặc Ủy ban nhân dân cấp tỉnh thành lập, có thể giao 01 Lãnh đạo đơn vị chuyên trách về an toàn thông tin / Sở Thông tin và Truyền thông phụ trách công tác bảo đảm an toàn thông tin làm nhiệm vụ Chủ tịch hội đồng;

(ii) Trường hợp Ủy ban nhân dân cấp huyện có đủ năng lực, được Ủy ban nhân dân cấp tỉnh quyết định làm chủ quản hệ thống thông tin, Hội đồng thẩm định độc lập do Ủy ban nhân dân cấp huyện thành lập, có thể giao 01 Lãnh đạo Ủy ban nhân dân huyện phụ trách công tác công nghệ thông tin/an toàn thông tin hoặc mời đại diện Lãnh đạo Sở Thông tin và Truyền thông phụ trách công tác bảo đảm an toàn thông tin làm nhiệm vụ Chủ tịch hội đồng.

2.4.2. Về các thành viên Hội đồng thẩm định

(1) Các thành viên nòng cốt là các công chức hoặc viên chức được giao nhiệm vụ phụ trách về an toàn thông tin của đơn vị chuyên trách về an toàn thông tin, độc lập với các công chức hoặc viên chức thuộc bộ phận/đơn vị được giao nhiệm vụ vận hành hệ thống thông tin;

(2) Mời bổ sung một số thành viên độc lập là cán bộ phụ trách về an toàn thông tin tại đơn vị chuyên trách về an toàn thông tin các bộ, ngành khác hoặc Văn phòng tỉnh ủy, Công an tỉnh, Bộ chỉ huy quân sự tỉnh tại địa phương… hoặc một số chuyên gia an toàn thông tin độc lập tại các doanh nghiệp công nghệ thông tin/an toàn thông tin (nếu cần).

2.4.3. Về trình độ chuyên môn của các thành viên Hội đồng thẩm định

Đơn vị chuyên trách về an toàn thông tin cân nhắc, lựa chọn theo phương án như sau:

(1) Các viên chức có chức danh nghề nghiệp an toàn thông tin tối thiểu hạng III trở lên theo quy định tại Thông tư số 08/2022/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông quy định mã số, tiêu chuẩn chức danh nghề nghiệp và xếp lương đối với viên chức chuyên ngành công nghệ thông tin, an toàn thông tin hoặc;

(2) Người có trình độ chuyên môn tối thiểu là đại học các chuyên ngành về an toàn thông tin hoặc các chuyên ngành về công nghệ thông tin nhưng có hiểu biết về kiến trúc an toàn thông tin (được đào tạo các kiến thức có liên quan hoặc đã từng tham gia thực hiện các nhiệm vụ, chương trình, đề tài nghiên cứu khoa học, đề án, dự án… về an toàn thông tin hoặc công nghệ thông tin có cấu phần về an toàn thông tin) hoặc có kinh nghiệm về đánh giá an toàn phần mềm / triển khai an toàn hệ thống thông tin / vận hành an toàn hệ thống theo quy định tại Thông tư số 17/2021/TT-BTTTT ngày 30/11/2021 của Bộ trưởng Bộ Thông tin và Truyền thông sửa đổi, bổ sung một số điều Thông tư số 11/2015/TT-BTTTT ngày 05 tháng 5 năm 2015 của Bộ Thông tin và Truyền thông Quy định Chuẩn kỹ năng nhân lực công nghệ thông tin chuyên nghiệp.

2.4.4. Báo cáo thẩm định hồ sơ đề xuất cấp độ của Hội đồng thẩm định

Vận dụng mẫu Văn bản ý kiến thẩm định, theo Mẫu số 04 được ban hành kèm theo Nghị định số 85/2016/NĐ-CP, gửi chủ quản hệ thống thông tin.

2.5. Thời gian thẩm định hồ sơ đề xuất cấp độ

a) Đối với hệ thống thông tin được đề xuất cấp độ 1 hoặc 2: Theo quy định tại khoản 2 Điều 17 Nghị định số 85/2016/NĐ-CP, thời gian xử lý phê duyệt (trong đó có thẩm định) tối đa là 07 ngày làm việc kể từ ngày nhận đủ hồ sơ hợp lệ.

b) Đối với hệ thống thông tin được đề xuất cấp độ 3, 4 hoặc 5 theo quy định tại khoản 2 Điều 16 Nghị định số 85/2016/NĐ-CP:

- Đối với hệ thống thông tin đề xuất cấp độ 3: Thời gian thẩm định tối đa là 15 ngày kể từ ngày nhận đủ hồ sơ hợp lệ;

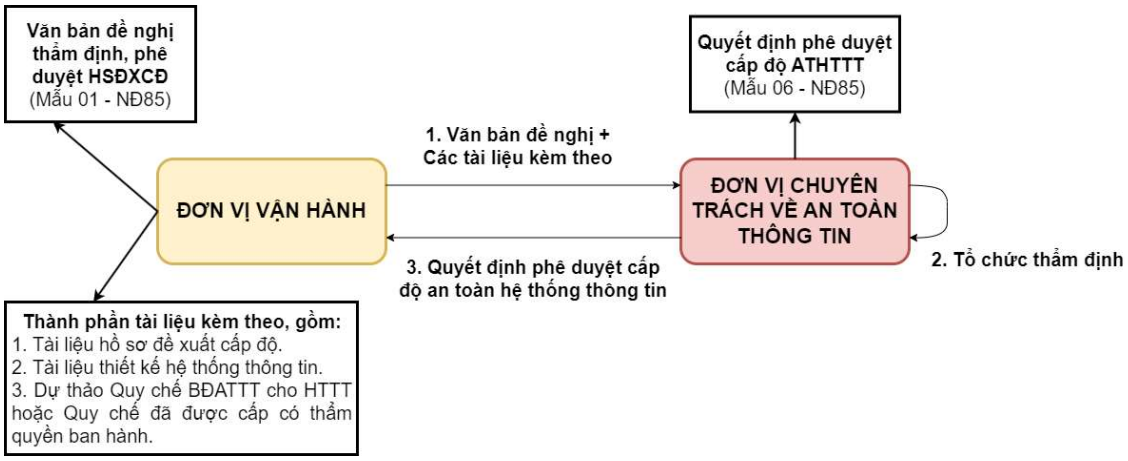
- Đối với hệ thống thông tin đề xuất cấp độ 4 hoặc cấp độ 5: Thời gian thẩm định tối đa là 30 ngày kể từ ngày nhận đủ hồ sơ hợp lệ.

Lưu ý: Trường hợp sau khi tổ chức thẩm định, hồ sơ đề xuất cấp độ của hệ thống thông tin được đánh giá chưa phù hợp, cần được điều chỉnh hoặc bổ sung, hoàn thiện, thời gian tổ chức thẩm định sẽ được tính lại kể từ thời điểm đơn vị thẩm định nhận được hồ sơ hoàn thiện.

3. Quy trình thẩm định, phê duyệt cấp độ

3.1. Đối với hệ thống thông tin đề xuất cấp độ 1 hoặc cấp độ 2

3.1.1. Sơ đồ quy trình



Hình 10. Quy trình thẩm định, phê duyệt cấp độ an toàn thông tin cấp độ 1, 2

3.1.2. Trình tự thực hiện

a) Bước 1. Gửi thẩm định hồ sơ đề xuất cấp độ:

Sau khi hoàn thành việc xây dựng hồ sơ đề xuất cấp độ, đơn vị vận hành hệ thống thông tin gửi hồ sơ đề nghị thẩm định, phê duyệt cấp độ an toàn thông tin[61] tới đơn vị chuyên trách về an toàn thông tin hoặc đơn vị được chủ quản hệ thống thông tin giao nhiệm vụ thẩm định, phê duyệt cấp độ an toàn thông tin để tổ chức thẩm định và phê duyệt.

b) Bước 2. Tổ chức thẩm định, phê duyệt cấp độ an toàn thông tin:

Đơn vị chuyên trách về an toàn thông tin hoặc đơn vị được chủ quản hệ thống thông tin giao nhiệm vụ thẩm định, phê duyệt cấp độ an toàn thông tin:

- Thực hiện thẩm định hồ sơ đề xuất cấp độ theo quy định (hình thức thẩm định xem chi tiết tại **Mục 2.2 và 2.4 Chương 5** ở trên);

- Có Văn bản ý kiến thẩm định (theo Mẫu số 04 ban hành kèm theo Nghị định số 85/2016/NĐ-CP) gửi đơn vị vận hành hệ thống thông tin.

Trên cơ sở kết quả thẩm định:

- Trường hợp hồ sơ đề xuất cấp độ đã được thuyết minh phù hợp với cấp độ đề xuất và đủ điều kiện phê duyệt cấp độ an toàn thông tin, đơn vị đã thẩm định hồ sơ đề xuất cấp độ tiến hành ban hành quyết định phê duyệt cấp độ an toàn thông tin đối với hệ thống thông tin (theo Mẫu số 06 Nghị định số 85/2016/NĐ-CP), gửi báo cáo chủ quản hệ thống thông tin theo quy định;

- Trường hợp hồ sơ đề xuất cấp độ được thuyết minh chưa phù hợp với cấp độ đề xuất, đơn vị vận hành hệ thống thông tin cần thuyết minh bổ sung hoặc giải trình, làm rõ đối với các nội dung được đánh giá không đạt, gửi lại hồ

[61] Thành phần hồ sơ xem **Mục 2.1 Chương 5** ở trên.

sơ để đơn vị thẩm định để tiếp tục thực hiện. Thời gian giải quyết được tính lại kể từ thời điểm đơn vị thẩm định nhận được hồ sơ đầy đủ, hoàn thiện.

Lưu ý:

(1) Việc tham mưu trình phê duyệt đề xuất cấp độ sẽ do 01 đơn vị trực thuộc đơn vị thẩm định thực hiện (không phải bộ phận được phân công nhiệm vụ vận hành hệ thống thông tin nếu đơn vị thẩm định đồng thời là đơn vị vận hành hệ thống thông tin);

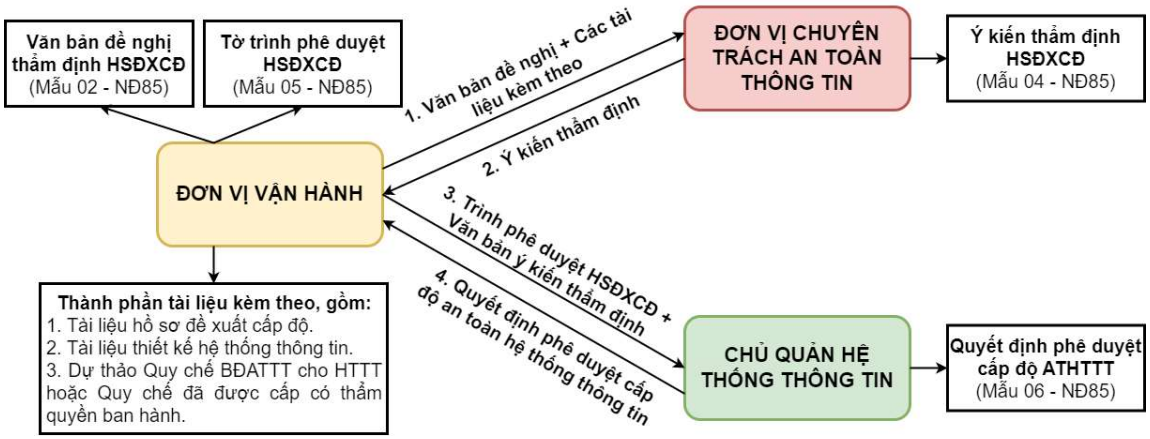
(2) Trước khi Lãnh đạo đơn vị thẩm định ký, ban hành quyết định phê duyệt cấp độ an toàn thông tin, quy chế bảo đảm an toàn thông tin cho hệ thống thông tin phải được cấp có thẩm quyền phê duyệt, ban hành.

3.1.3. Thời gian giải quyết

Tối đa 07 ngày làm việc kể từ ngày nhận đủ hồ sơ hợp lệ (bao gồm cả thời gian tổ chức thẩm định và phê duyệt cấp độ).

3.2. Đối với hệ thống thông tin đề xuất cấp độ 3

3.2.1. Sơ đồ quy trình



Hình 11. Quy trình thẩm định, phê duyệt cấp độ an toàn thông tin cấp độ 3

3.2.2. Trình tự thực hiện

a) Bước 1. Gửi thẩm định hồ sơ đề xuất cấp độ:

Sau khi hoàn thành việc xây dựng hồ sơ đề xuất cấp độ, đơn vị vận hành hệ thống thông tin gửi hồ sơ đề nghị thẩm định[62] tới đơn vị chuyên trách về an toàn thông tin hoặc đơn vị được chủ quản hệ thống thông tin giao nhiệm vụ thẩm định hồ sơ đề xuất cấp độ để tổ chức thẩm định.

b) Bước 2. Tổ chức thẩm định:

Đơn vị chuyên trách về an toàn thông tin hoặc đơn vị được chủ quản hệ thống thông tin giao nhiệm vụ thẩm định hồ sơ đề xuất cấp độ an toàn thông tin:

- Thực hiện thẩm định hồ sơ đề xuất cấp độ theo quy định;

[62] Thành phần hồ sơ xem **Mục 2.1 Chương 5** ở trên.

- Có Văn bản ý kiến thẩm định (theo Mẫu số 04 ban hành kèm theo Nghị định số 85/2016/NĐ-CP) gửi đơn vị vận hành hệ thống thông tin.

Trên cơ sở kết quả thẩm định, trường hợp hồ sơ đề xuất cấp độ được thuyết minh chưa phù hợp với cấp độ đề xuất, đơn vị vận hành hệ thống thông tin cần thuyết minh bổ sung hoặc giải trình, làm rõ các nội dung được đánh giá không đạt, gửi lại hồ sơ để đơn vị thẩm định tiếp tục thực hiện. Thời gian giải quyết được tính lại từ thời điểm đơn vị thẩm định nhận được hồ sơ đầy đủ, hoàn thiện.

c) Bước 3. Trình phê duyệt:

Trên cơ sở kết quả thẩm định, trường hợp hồ sơ đề xuất cấp độ của hệ thống thông tin đã được thuyết minh phù hợp với cấp độ đề xuất và đủ điều kiện phê duyệt cấp độ an toàn thông tin, đơn vị vận hành hệ thống thông tin hoàn thiện hồ sơ đề xuất cấp độ, trình chủ quản hệ thống thông tin xem xét phê duyệt.

Hồ sơ trình chủ quản hệ thống thông tin phê duyệt đề xuất cấp độ gồm:

(1) Tờ trình chủ quản hệ thống thông tin phê duyệt hồ sơ đề xuất cấp độ của đơn vị vận hành (theo Mẫu số 05 ban hành kèm theo Nghị định số 85/2016/NĐ-CP);

(2) Văn bản ý kiến thẩm định hồ sơ đề xuất cấp độ đã được đơn vị thẩm định hồ sơ đề xuất cấp độ ban hành (theo Mẫu số 04 ban hành kèm theo Nghị định số 85/2016/NĐ-CP);

(3) Các tài liệu khác kèm theo, phục vụ phê duyệt (như tại bước gửi thẩm định hồ sơ đề xuất cấp độ), trong đó, quy chế bảo đảm an toàn thông tin cho hệ thống đã phải được cấp có thẩm quyền phê duyệt, ban hành.

d) Bước 4. Phê duyệt cấp độ an toàn thông tin:

Chủ quản hệ thống thông tin xem xét, ban hành quyết định phê duyệt cấp độ an toàn hệ thống thông tin (theo Mẫu số 06 Nghị định số 85/2016/NĐ-CP).

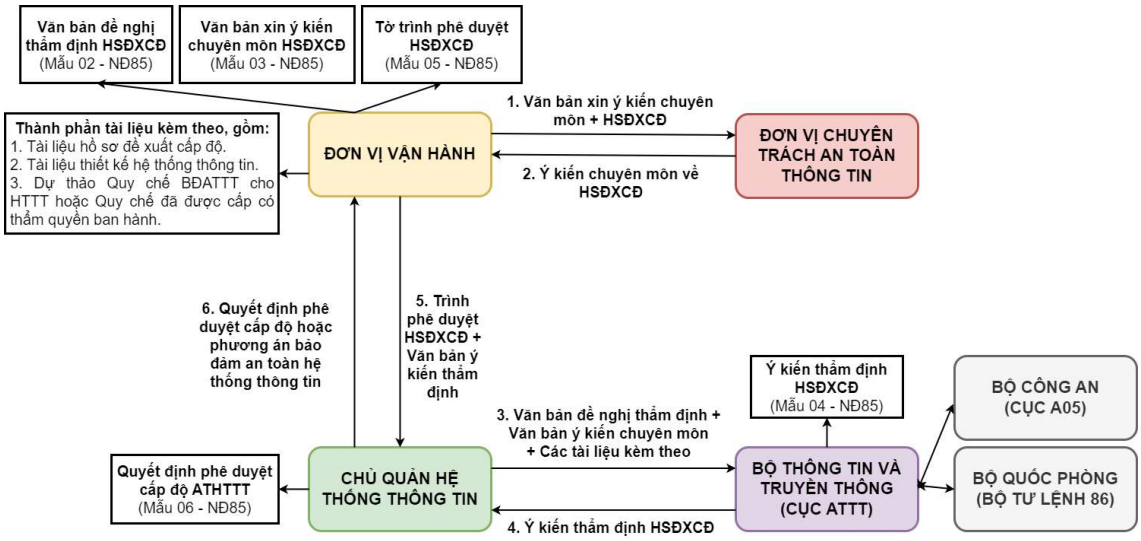
3.2.3. Thời gian giải quyết

- Thời gian thẩm định: Tối đa 15 ngày kể từ ngày nhận đủ hồ sơ hợp lệ;

- Thời gian phê duyệt: Tối đa 07 ngày làm việc kể từ ngày nhận đủ hồ sơ hợp lệ.

3.3. Đối với hệ thống thông tin đề xuất cấp độ 4 hoặc cấp độ 5

3.3.1. Sơ đồ quy trình



Hình 12. Quy trình thẩm định, phê duyệt cấp độ an toàn thông tin cấp độ 4, 5

3.3.2. Trình tự thực hiện

a) Bước 1. Gửi xin ý kiến chuyên môn về hồ sơ đề xuất cấp độ:

Sau khi hoàn thành việc xây dựng hồ sơ đề xuất cấp độ, đơn vị vận hành hệ thống thông tin gửi đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin hồ sơ đề nghị cho ý kiến chuyên môn về an toàn thông tin đối với hồ sơ đề xuất cấp độ, gồm:

- Văn bản xin ý kiến chuyên môn về hồ sơ đề xuất cấp độ (theo Mẫu số 03 được ban hành kèm theo Nghị định số 85/2016/NĐ-CP);

- Các tài liệu có liên quan kèm theo, phục vụ cho ý kiến chuyên môn (xem **Mục 2.1 Chương 5** ở trên).

b) Bước 2. Cho ý kiến chuyên môn về hồ sơ đề xuất cấp độ:

Đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin:

- Cho ý kiến chuyên môn về hồ sơ đề xuất cấp độ theo quy định và;

- Có Văn bản cho ý kiến góp ý chuyên môn về hồ sơ đề xuất cấp độ gửi đơn vị vận hành hệ thống thông tin.

Văn bản ý kiến chuyên môn về an toàn thông tin đối với hồ sơ đề xuất cấp độ cần làm rõ các nội dung sau đây (hướng dẫn cho ý kiến chi tiết áp dụng hướng dẫn tại các Mục 2.3.2, 2.3.3, 2.3.4 và 2.3.5 Chương 5 ở trên):

(1) Sự phù hợp về việc đề xuất cấp độ;

(2) Sự phù hợp của phương án bảo đảm an toàn hệ thống thông tin trong tài liệu thiết kế hệ thống thông tin;

(3) Sự phù hợp của phương án bảo đảm an toàn hệ thống thông tin trong quá trình vận hành hệ thống theo cấp độ tương ứng.

Trên cơ sở ý kiến chuyên môn của đơn vị chuyên trách về an toàn thông tin:

- Trường hợp hồ sơ đề xuất cấp độ của hệ thống thông tin được thuyết minh chưa phù hợp với cấp độ đề xuất, đơn vị vận hành hệ thống thông tin cần thuyết minh bổ sung hoặc giải trình, làm rõ đối với các nội dung được cho ý kiến đánh giá chưa đáp ứng (không đạt) và gửi lại hồ sơ cho đơn vị chuyên trách về an toàn thông tin để tiếp tục cho ý kiến chuyên môn theo quy định;

- Trường hợp hồ sơ đề xuất cấp độ của hệ thống thông tin đã được thuyết minh phù hợp với cấp độ đề xuất và đủ điều kiện trình chủ quản hệ thống thông tin xem xét gửi cơ quan có thẩm quyền thẩm định, đơn vị vận hành hệ thống thông tin hoàn thiện hồ sơ đề xuất cấp độ, trình chủ quản hệ thống thông tin xem xét.

c) Bước 3. Gửi thẩm định hồ sơ đề xuất cấp độ:

Chủ quản hệ thống thông tin gửi hồ sơ đề nghị thẩm định hồ sơ đề xuất cấp độ tới cơ quan có thẩm quyền để chủ trì tổ chức thẩm định theo quy định, trong đó:

- Đối với hệ thống thông tin không phạm vi quản lý của Bộ Quốc phòng, Bộ Công an: Cơ quan có thẩm quyền chủ trì thẩm định là Bộ Thông tin và Truyền thông;

- Đối với hệ thống thông tin thuộ phạm vi quản lý của Bộ Quốc phòng: Cơ quan có thẩm quyền chủ trì thẩm định là Bộ Quốc phòng;

- Đối với hệ thống thông tin thuộ phạm vi quản lý của Bộ Công an: Cơ quan có thẩm quyền chủ trì thẩm định là Bộ Công an.

d) Bước 4. Tổ chức thẩm định:

- Bộ Thông tin và Truyền thông chủ trì, phối hợp với Bộ Quốc phòng, Bộ Công an và các bộ, ngành liên quan thực hiện thẩm định hồ sơ đề xuất cấp độ đối với hồ sơ đề xuất cấp độ của hệ thống thông tin không phải do Bộ Quốc phòng, Bộ Công an quản lý;

- Bộ Quốc phòng chủ trì, phối hợp với Bộ Thông tin và Truyền thông và bộ, ngành liên quan thực hiện thẩm định hồ sơ đề xuất cấp độ đối với hệ thống thông tin do Bộ Quốc phòng quản lý;

- Bộ Công an chủ trì, phối hợp với Bộ Thông tin và Truyền thông và bộ, ngành liên quan thực hiện thẩm định hồ sơ đề xuất cấp độ đối với hệ thống thông tin do Bộ Công an quản lý.

Kết quả thẩm định: Văn bản ý kiến thẩm định của cơ quan có thẩm quyền (theo Mẫu số 04 được ban hành kèm theo Nghị định số 85/2016/NĐ-CP).

Trên cơ sở kết quả thẩm định, trường hợp hồ sơ đề xuất cấp độ của hệ thống thông tin được thuyết minh chưa phù hợp với cấp độ đề xuất, chủ quản hệ thống thông tin giao đơn vị vận hành hệ thống thông tin thuyết minh bổ sung hoặc giải trình, làm rõ đối với các nội dung được đánh giá không đạt và gửi lại hồ sơ cho cơ quan thẩm định để tiếp tục tiến hành quy trình thẩm định theo quy

định. Thời gian giải quyết được tính lại từ thời điểm cơ quan thẩm định nhận được hồ sơ đầy đủ, hoàn thiện.

đ) Bước 5. Trình phê duyệt:

Trên cơ sở kết quả thẩm định, trường hợp hồ sơ đề xuất cấp độ của hệ thống thông tin đã được thuyết minh phù hợp với cấp độ đề xuất và đủ điều kiện phê duyệt cấp độ an toàn thông tin (đối với hệ thống thông tin đề xuất cấp độ 4) hoặc đủ điều kiện phê duyệt phương án bảo đảm an toàn hệ thống thông tin (đối với hệ thống thông tin đề xuất cấp độ 5), đơn vị vận hành hệ thống thông tin hoàn thiện hồ sơ đề xuất cấp độ, trình chủ quản hệ thống thông tin xem xét phê duyệt.

Hồ sơ trình chủ quản hệ thống thông tin phê duyệt bao gồm:

(1) Tờ trình chủ quản hệ thống thông tin phê duyệt hồ sơ đề xuất cấp độ của đơn vị vận hành (theo Mẫu số 05 ban hành kèm theo Nghị định số 85/2016/NĐ-CP);

(2) Văn bản ý kiến chuyên môn về hồ sơ đề xuất cấp độ của đơn vị chuyên trách về an toàn thông tin;

(3) Văn bản ý kiến thẩm định hồ sơ đề xuất cấp độ của cơ quan có thẩm quyền thẩm định (theo Mẫu số 04 ban hành kèm theo Nghị định số 85/2016/NĐ-CP);

(4) Các tài liệu khác kèm theo, phục vụ phê duyệt (như tại bước gửi thẩm định hồ sơ đề xuất cấp độ), trong đó, quy chế bảo đảm an toàn thông tin cho hệ thống đã phải được cấp có thẩm quyền phê duyệt, ban hành.

e) Bước 6. Phê duyệt cấp độ hoặc phương án bảo đảm an toàn thông tin:

- Đối với hệ thống thông tin được đề xuất cấp độ 4: Chủ quản hệ thống thông tin xem xét, ký ban hành quyết định phê duyệt cấp độ an toàn hệ thống thông tin (theo Mẫu số 06 được ban hành kèm theo Nghị định số 85/2016/NĐ-CP);

- Đối với hệ thống thông tin được đề xuất cấp độ 5: Chủ quản hệ thống thông tin xem xét, ký ban hành quyết định phê duyệt phương án bảo đảm an toàn thông tin (theo Mẫu số 07 được ban hành kèm theo Nghị định số 85/2016/NĐ-CP).

3.2.3. Thời gian giải quyết

- Thời gian thẩm định: Tối đa 30 ngày kể từ ngày nhận đủ hồ sơ hợp lệ;

- Thời gian phê duyệt: Tối đa 07 ngày làm việc kể từ ngày nhận đủ hồ sơ hợp lệ.

4. Thời điểm phê duyệt cấp độ an toàn thông tin

Theo quy định tại Điều 15 Thông tư số 12/2022/TT-BTTTT, 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.

Tuy nhiên, theo khoản 6 Điều 9 Thông tư số 12/2022/TT-BTTTT, "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 trước khi đưa vào vận hành, khai thác", do đó, hệ thống thông tin phải được phê duyệt cấp độ an toàn thông tin trước *khi đưa vào vận hành, khai thác*.

5. Điều chỉnh, cập nhật nội dung hồ sơ đề xuất cấp độ

Đối với các hệ thống thông tin đang vận hành, khai thác, đã được phê duyệt cấp độ, trong trường hợp:

- Qua rà soát, nhận thấy cần điều chỉnh, cập nhật nội dung hồ sơ đề xuất cấp độ (điều chỉnh cấp độ hoặc cập nhật, hoàn thiện phương án bảo đảm an toàn thông tin), hoặc;

- Khi hệ thống thông tin được nâng cấp, mở rộng.

Đơn vị vận hành hệ thống thông tin cần cập nhật, hoàn thiện hồ sơ đề xuất cấp độ, phối hợp đơn vị chuyên trách về an toàn thông tin hoặc đơn vị được chủ quản hệ thống thông tin giao thẩm định hồ sơ đề xuất cấp độ xem xét:

(1) Trong tường hợp cập nhật, hoàn hiện nội dung hồ sơ đề xuất cấp độ nhưng không làm thay đổi phương án bảo đảm an toàn thông tin và cấp độ an toàn thông tin: Đơn vị chuyên trách về an toàn thông tin hoặc đơn vị được chủ quản hệ thống thông tin giao thẩm định hồ sơ đề xuất cấp độ lưu hồ sơ để theo dõi;

(2) Trong trường hợp điều chỉnh, cập nhật nội dung hồ sơ đề xuất cấp độ làm thay đổi phương án bảo đảm an toàn thông tin nhưng không làm thay đổi cấp độ an toàn thông tin của hệ thống thông tin: Thực hiện lại quy trình thẩm định, phê duyệt cấp độ an toàn thông tin hoặc phương án bảo đảm an toàn thông tin. Khi đó, tại quyết định phê duyệt cấp độ / phương án bảo đảm an toàn thông tin (Mẫu số 06 và Mẫu số 07 ban hành kèm theo Nghị định số 85/2016/NĐ-CP):

- Mục căn cứ: Ghi rõ phiên bản của hồ sơ đề xuất cấp độ (kèm theo Tờ trình số … ngày … của …);

- Mục Điều khoản thi hành: Bổ sung nội dung "Quyết định này có hiệu lực kể từ ngày ký, thay thế Quyết định số … ngày … của … về việc …".

6. Trình Thủ tướng Chính phủ phê duyệt, đưa hệ thống thông tin vào danh mục hệ thống thông tin cấp độ 5

a) Căn cứ quy định tại điểm c khoản 3 Điều 14 Nghị định số 85/2016/NĐ-CP, đối với hệ thống thông tin được đề xuất là cấp độ 5, trên cơ sở kết quả thẩm định hồ sơ đề xuất cấp độ, Bộ Thông tin và Truyền thông chủ trì, phối hợp với Bộ Quốc phòng, Bộ Công an và bộ, ngành có liên quan trình Thủ tướng Chính phủ phê duyệt danh mục hệ thống thông tin cấp độ 5.

Thực hiện quy định trên, sau khi có kết quả thẩm định hồ sơ đề xuất cấp độ và hệ thống thông tin đủ điều kiện để được phê duyệt là hệ thống thông tin cấp độ 5, chủ quản hệ thống thông tin:

- Tiến hành phê duyệt phương án bảo đảm an toàn thông tin;

- Hoàn thiện hồ sơ, gửi Bộ Thông tin và Truyền thông (04 bộ hồ sơ) để trình Thủ tướng Chính phủ phê duyệt, đưa hệ thống thông tin vào danh mục hệ thống thông tin cấp độ 5 (Danh mục hệ thống thông tin quan trọng quốc gia).

b) Thành phần hồ sơ gửi Bộ Thông tin và Truyền thông gồm có:

- Văn bản đề nghị trình Thủ tướng Chính phủ phê duyệt, đưa hệ thống thông tin vào danh mục hệ thống thông tin cấp độ 5;

- Văn bản ý kiến thẩm định hồ sơ đề xuất cấp độ đã được cơ quan có thẩm quyền thẩm định hồ sơ đề xuất cấp độ ban hành;

- Quyết định phê duyệt phương ấn bảo đảm an toàn thông tin đã được chủ quản hệ thống thông tin ban hành;

- Hồ sơ đề xuất cấp độ hoàn thiện và các tài liệu khác kèm theo (như tại bước trình phê duyệt hồ sơ đề xuất cấp độ an toàn thông tin).

c) Khi nhận được hồ sơ đầy đủ, hợp lệ, Bộ Thông tin và Truyền thông sẽ chủ trì, gửi lấy ý kiến thống nhất của Bộ Quốc phòng, Bộ Công an và các bộ, ngành có liên quan trước khi trình Thủ tướng Chính phủ xem xét, ký ban hành Quyết định phê duyệt, đưa hệ thống thông tin vào danh mục hệ thống thông tin cấp độ 5 (danh mục hệ thống thông tin quan trọng quốc gia).

7. Trình Thủ tướng Chính phủ phê duyệt, đưa hệ thống thông tin ra khỏi danh mục hệ thống thông tin cấp độ 5

a) Trường hợp hệ thống thông tin cấp độ 5 cần điều chỉnh, hạ cấp độ an toàn thông tin, sau khi đơn vị vận hành hoàn thiện việc cập nhật, điều chỉnh hồ sơ đề xuất cấp độ, chủ quản hệ thống thông tin gửi Bộ Thông tin và Truyền thông (04 bộ hồ sơ) để chủ trì, phối hợp các cơ quan, tổ chức có liên quan cho ý kiến.

b) Thành phần hồ sơ gửi Bộ Thông tin và Truyền thông gồm có:

- Văn bản đề nghị trình Thủ tướng Chính phủ phê duyệt, đưa hệ thống thông tin ra khỏi danh mục hệ thống thông tin cấp độ 5, trong đó thuyết minh làm rõ căn cứ điều chỉnh, hạ cấp độ an toàn thông tin;

- Bản chụp Quyết định của Thủ tương Chính phê duyệt, đưa hệ thống thông tin vào danh mục hệ thống thông tin cấp độ 5;

- Hồ sơ đề xuất cấp độ theo đề xuất cấp độ mới và các tài liệu khác kèm theo (như tại bước gửi thẩm định hồ sơ đề xuất cấp độ).

c) Khi nhận được hồ sơ đầy đủ, hợp lệ, Bộ Thông tin và Truyền thông sẽ chủ trì, gửi lấy ý kiến thống nhất của Bộ Quốc phòng, Bộ Công an và bộ, ngành có liên quan. Trường hợp tất cả các cơ quan thống nhất việc hạ cấp độ an toàn thông tin của hệ thống thông tin, Bộ Thông tin và Truyền thông sẽ trình Thủ tướng Chính phủ xem xét, ký ban hành Quyết định *bãi bỏ Quyết định* đưa hệ thống thông tin vào danh mục hệ thống thông tin cấp độ 5 (danh mục hệ thống thông tin quan trọng quốc gia).

TỔNG KẾT CHƯƠNG 5

1. Hệ thống thông tin được đầu tư xây dựng mới hoặc mở rộng, nâng cấp *phải được phê duyệt cấp độ an toàn thông tin và triển khai đầy đủ phương án bảo đảm an toàn thông tin theo hồ sơ đề xuất cấp độ đã được phê duyệt trước khi đưa vào vận hành, khai thác.*

2. Đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin có trách nhiệm: (1) thẩm định hồ sơ đề xuất cấp độ của hệ thống thông tin được đề xuất cấp độ 1, 2, 3; (2) phê duyệt cấp độ an toàn thông tin của hệ thống thông tin được đề xuất cấp độ 1, 2; (3) cho ý kiến chuyên môn đối với hồ sơ đề xuất cấp độ của hệ thống thông tin được đề xuất cấp độ 4, 5.

3. Chủ quản hệ thống thông tin có trách nhiệm: (1) phê duyệt cấp độ an toàn thông tin của hệ thống thông tin được đề xuất cấp độ 3, 4; (2) phê duyệt phương án bảo đảm an toàn thông tin của hệ thống thông tin được đề xuất cấp độ 5.

4. Hồ sơ đề xuất cấp độ của hệ thống thông tin đang vận hành, khai thác, đã được phê duyệt cấp độ cần được điều chỉnh cấp độ hoặc cập nhật, hoàn thiện khi:

- Qua rà soát, nhận thấy cần điều chỉnh cấp độ hoặc điều chỉnh, cập nhật nội dung hồ sơ đề xuất cấp độ cho phù hợp với phương án bảo đảm an toàn thông tin đã được cập nhật, hoàn thiện, hoặc;
- Khi hệ thống thông tin được nâng cấp, mở rộng.

Khi đó, đơn vị vận hành hệ thống thông tin phối hợp đơn vị chuyên trách về an toàn thông tin hoặc đơn vị được chủ quản hệ thống thông tin giao thẩm định hồ sơ đề xuất cấp độ xem xét tổ chức thẩm định, phê duyệt lại cấp độ nếu cần thiết.

Chương 6.
Chế độ báo cáo

Chế độ báo cáo trong lĩnh vực bảo đảm an toàn hệ thống thông tin theo cấp độ được quy định chi tiết tại các Điều 13 và 14 Thông tư số 12/2022/TT-BTTTT nhằm làm rõ các quy định chung về chế độ báo cáo, nội dung báo cáo tại khoản 4 Điều 22 Nghị định số 85/2016/NĐ-CP và đồng bộ với các quy định tại Nghị định số 09/2019/NĐ-CP ngày 24/01/2019 của Chính phủ về chế độ báo cáo của các cơ quan nhà nước, theo đó, việc thực hiện chế độ báo cáo định kỳ hoặc đột xuất khi có yêu cầu là trách nhiệm của:

(1) Đơn vị vận hành hệ thống thông tin phải báo cáo chủ quản hệ thống thông tin hoặc cơ quan quản lý nhà nước chuyên ngành có thẩm quyền;

(2) Chủ quản hệ thống thông tin báo cáo Bộ Thông tin và Truyền thông.

Chương này sẽ hướng dẫn chi tiết về chế độ báo cáo trong lĩnh vực bảo đảm an toàn hệ thống thông tin theo cấp độ.

1. Các quy định chung

Căn cứ các quy định tại Điều 13 Thông tư số 12/2022/TT-BTTTT:

1.1. Phương thức gửi, nhận báo cáo

Có 03 phương thức chính để gửi, nhận báo cáo trong công tác bảo đảm an toàn hệ thống thông tin theo cấp độ, cụ thể:

(1) Gửi qua hệ thống quản lý văn bản và điều hành: Định kỳ hoặc đột xuất khi có yêu cầu bằng văn bản;

(2) Gửi qua hệ thống phần mềm báo cáo do Bộ Thông tin và Truyền thông triển khai: Cập nhật thường xuyên, liên tục thông tin về tình hình thực hiện bảo đảm an toàn thông tin theo cấp độ đối với các hệ thống thông tin thuộc phạm vi quản lý trên *Nền tảng hỗ trợ quản lý bảo đảm an toàn hệ thống thông tin theo cấp độ*;

(3) Gửi qua hệ thống thư điện tử: Định kỳ hoặc đột xuất khi có yêu cầu bằng văn bản.

Ngoài ra, các đơn vị có thể thực hiện gửi, nhận báo cáo theo các phương thức khác theo quy định của pháp luật.

1.2. Tần suất thực hiện

a) Định kỳ hàng năm;

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

1.3. 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.

1.4. 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.

2. Nội dung báo cáo

2.1. Quy định về nội dung báo cáo

Căn cứ các quy định tại Điều 14 Thông tư số 12/2022/TT-BTTTT, nội dung báo cáo bao gồm các thông tin sau đây:

(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 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 cấp độ an toàn thông tin 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 về quyết định phê duyệt cấp độ an toàn thông tin, 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 về 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.

2.2. Mẫu báo cáo

2.2.1. Thông tin chung

- Tổng số hệ thống thông tin thuộc phạm vi quản lý: …;

- Tổng số hệ thống thông tin đã được phân loại (đã xác định được loại hình hệ thống thông tin): …;

- Tổng số hệ thống thông tin đã xây dựng hồ sơ đề xuất cấp độ: …;

- Tổng số hệ thống thông tin đã được thẩm định hồ sơ đề xuất cấp độ đã được thẩm định: …;

- Tổng số hệ thống thông tin đã được phê duyệt cấp độ: …;

- Tổng số hệ thống thông tin đã phê duyệt cấp độ được kiểm tra, đánh giá an toàn thông tin định kỳ theo quy định: …;

- Dự kiến thời gian hoàn thành phê duyệt đề xuất cấp độ an toàn hệ thống thông tin đối với tất cả các hệ thống thông tin thuộc phạm vi quản lý: …

2.2.2. Thông tin về chủ quản hệ thống thông tin và đơn vị chuyên trách về an toàn thông tin

a) Thông tin về chủ quản hệ thống thông tin:

(1) Tên chủ quản hệ thống thông tin: Ghi rõ tên cơ quan được xác định là chủ quản hệ thống thông tin;

(2) Quy định chức năng, nhiệm vụ và quyền hạn: Ghi rõ thông tin văn bản quy định chức năng, nhiệm vụ và quyền hạn (nếu có) của cơ quan chủ quản hệ thống thông tin. Trường hợp không có thì để trống;

(3) Người đại diện, chức vụ: Ghi rõ họ và tên, chức vụ của người đứng đầu cơ quan được xác định là chủ quản hệ thống thông tin;

(4) Địa chỉ liên lạc của cơ quan chủ quản hệ thống thông tin;

(5) Thông tin liên hệ bao gồm: Số điện thoại, thư điện tử của cơ quan được xác định là chủ quản hệ thống thông tin.

b) Thông tin về đơn vị chuyên trách về an toàn thông tin:

(1) Tên đơn vị chuyên trách về an toàn thông tin: Ghi rõ tên cơ quan/đơn vị được chủ quản hệ thống thông tin giao nhiệm vụ là đơn vị chuyên trách về an toàn thông tin;

(2) Quy định chức năng, nhiệm vụ và quyền hạn: Ghi rõ thông tin văn bản quy định chức năng, nhiệm vụ và quyền hạn của đơn vị chuyên trách về an toàn thông tin;

(3) Người đại diện, chức vụ: Ghi rõ họ và tên, chức vụ của người đứng đầu đơn vị chuyên trách về an toàn thông tin;

(4) Địa chỉ liên lạc của đơn vị chuyên trách về an toàn thông tin;

(5) Thông tin liên hệ bao gồm: Số điện thoại, thư điện tử của đơn vị chuyên trách về an toàn thông tin.

Trường hợp thuộc phạm vi quản lý có nhiều đơn vị có đủ năng lực, được quyết định là chủ quản hệ thống thông tin thì lần lượt báo cáo thông tin về từng chủ quản hệ thống thông tin và đơn vị chuyên trách về an toàn thông tin tương ứng.

2.2.3. Thông tin chi tiết về các hệ thống thông tin thuộc phạm vi quản lý

STT	Tên HTTT	Chủ quản HTTT	Đơn vị vận hành HTTT	Cấp độ đề xuất	Tình trạng phê duyệt cấp độ	Quyết định phê duyệt cấp độ	Quy chế bảo đảm ATTT cho hệ thống	Dự kiến thời điểm phê duyệt HSĐXCĐ	Đã triển khai đầy đủ PA BĐATTT	Dự kiến thời điểm triển khai đầy đủ PA BĐATTT	Đã kiểm tra, đánh giá ATTT
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
1	…	…	…	…	…	…	…	…	…	…	…

Chú thích:

- Cột (2), (3), (4) ghi tên các hệ thống thông tin, tên cơ quan chủ quản, tên đơn vị vận hành hệ thống thông tin;

- Cột (5) ghi cấp độ đề xuất đối với hệ thống thông tin: 1-5;

- Cột (6) ghi tình trạng phê duyệt cấp độ an toàn thông tin của hệ thống thông tin: "Đang dự thảo", "Đã gửi thẩm định", "Đã thẩm định", "Đã được phê duyệt";

- Cột (7) ghi thông tin số, ngày quyết định, tên cơ quan phê duyệt cấp độ nếu hệ thống thông tin đã được phê duyệt cấp độ;

- Cột (8) ghi thông tin số, ngày quyết định, tên cơ quan ban hành quy chế bảo đảm an toàn thông tin cho hệ thống (nếu có);

- Cột (9) ghi thời điểm dự kiến phê duyệt cấp độ (nếu hệ thống thông tin chưa được phê duyệt cấp độ);

- Cột (10) ghi tình trạng triển khai đầy đủ phương án bảo đảm an toàn thông tin theo cấp độ tương ứng: "Chưa triển khai", "Đã triển khai một số hạng mục", "Đã triển khai đầy đủ";

- Cột (11) ghi thời điểm dự kiến triển khai đầy đủ phương án bảo đảm an toàn thông tin theo cấp độ tương ứng.

- Cột (12) ghi tình trạng kiểm tra, đánh giá an toàn thông tin theo quy định: "Trước khi đưa vào sử dụng", "Định kỳ", hoặc ghi cả hai nếu đã thực hiện đầy đủ, để trống nếu chưa thực hiện.

3. Nền tảng hỗ trợ quản lý bảo đảm an toàn hệ thống thông tin theo cấp độ

Địa chỉ truy cập Nền tảng: https://capdo.ais.gov.vn.

Nền tảng hỗ trợ quản lý bảo đảm an toàn hệ thống thông tin theo cấp độ đã được Bộ Thông tin và Truyền thông khai trương ngày 30/11/2023 tại Hội thảo - Triển lãm "Ngày An toàn thông tin Việt Nam" năm 2023 với chủ đề: "An toàn dữ liệu trong thời đại điện toán đám mây (ĐTĐM) và trí tuệ nhân tạo (AI)" và được triển khai chính thức (miễn phí) theo Công văn số 387/CATTT-ATHTTT ngày 18/3/2024 của Cục An toàn thông tin về việc hướng dẫn sử dụng Nền tảng hỗ trợ quản lý bảo đảm an toàn hệ thống thông tin theo cấp độ.

Theo đó, đơn vị chuyên trách về công nghệ thông tin/an toàn thông tin của các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương cần tổ chức:

(1) Chỉ định và bố trí bộ phận, cán bộ chuyên trách về việc sử dụng, vận hành khai thác hiệu quả Nền tảng để phục vụ công tác quản lý nhà nước về an toàn thông mạng, bao gồm xây dựng, thẩm định, phê duyệt và giám sát, theo dõi tình hình thực thi hồ sơ đề xuất cấp độ của hệ thống thông tin.

(2) Rà soát việc đăng ký sử dụng Nền tảng theo danh sách tại Phụ lục II gửi kèm theo Công văn số 387/CATTT-ATHTTT nêu trên. Trường hợp chưa đăng ký tài khoản thì liên hệ với đầu mối hỗ trợ của Cục An toàn thông tin để đăng ký sử dụng Nền tảng.

Mỗi chủ quản hệ thống thông tin (bộ, ngành, địa phương) được cấp 01 tài khoản quản trị cho đơn vị chuyên trách về an toàn thông tin để sử dụng Nền tảng. Tài khoản quản trị này sẽ tạo và quản lý các tài khoản khác sử dụng cho các đơn vị trực thuộc bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân cấp tỉnh có quản lý, vận hành hệ thống thông tin.

(3) Nghiên cứu và hướng dẫn, đôn đốc các đơn vị vận hành hệ thống thông tin và các đơn vị liên quan sử dụng Nền tảng thông qua các tài liệu hướng dẫn theo Phụ lục I của Công văn số 387/CATTT-ATHTTT.

(4) Đăng ký Kênh thông tin trực tuyến để được Cục An toàn thông tin hỗ trợ trong quá trình vận hành, khai thác sử dụng Nền tảng, theo thông tin đăng ký tại Phụ lục I của Công văn số 387/CATTT-ATHTTT.

(5) Rà soát danh mục các hệ thống thông tin thuộc phạm vi quản lý và tạo tài khoản cho các đơn vị vận hành theo tài liệu hướng dẫn. Mỗi đơn vị vận hành hệ thống thông tin được tạo 01 tài khoản để quản lý toàn bộ các hệ thống thông tin thuộc phạm vi quản lý.

(6) Thông báo cho đơn vị vận hành việc tạo mới/cập nhật hệ thống thông tin và xây dựng hồ sơ đề xuất cấp độ sử dụng Nền tảng (bao gồm cả các hệ thống thông tin đã được phê duyệt cấp độ an toàn thông tin và các hệ thống

thông tin chuẩn bị xây dựng hồ sơ đề xuất cấp độ/phê duyệt cấp độ an toàn thông tin). Hoàn thành việc khai báo, cập nhật thông tin của các hệ thống thông tin đã phê duyệt cấp độ an toàn thông tin **trước ngày 30/5/2024**. Hoàn thành việc khai báo, cập nhật thông tin của các hệ thống chuẩn bị xây dựng hồ sơ đề xuất cấp độ/phê duyệt cấp độ an toàn thông tin **trước ngày 30/7/2024**.

(7) Thực hiện quy trình thẩm định hồ sơ đề xuất cấp độ và phê duyệt cấp độ an toàn thông tin theo quy định.

(8) Sử dụng Nền tảng thường xuyên, liên tục để theo dõi, kiểm tra, đôn đốc các đơn vị vận hành việc phê duyệt cấp độ an toàn thông tin và triển khai đầy đủ phương án bảo đảm an toàn hệ thống thông tin theo hồ sơ đề xuất cấp độ đã được phê duyệt.

(9) Theo Chỉ thị số 09/CT-TTg của Thủ tướng Chính phủ, Bộ Thông tin và Truyền thông sẽ sử dụng thông tin, số liệu được cập nhật trên Nền tảng để đánh giá, xếp hạng công tác bảo đảm an toàn hệ thống thông tin theo cấp độ của các bộ, ngành, địa phương và báo cáo Thủ tướng Chính phủ từ năm 2024.

Như vậy, trên cơ sở triển khai Nền tảng hỗ trợ quản lý bảo đảm an toàn hệ thống thông tin theo cấp độ, từ năm 2024, Bộ Thông tin và Truyền thông, các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ và Ủy ban nhân dân cấp tỉnh sẽ thống nhất triển khai chế độ báo cáo trong lĩnh vực bảo đảm an toàn hệ thống thông tin theo cấp độ thông qua Nền tảng này.

TỔNG KẾT CHƯƠNG 6

1. Trong lĩnh vực bảo đảm an toàn hệ thống thông tin theo cấp độ, chế độ báo cáo định kỳ hoặc đột xuất khi có yêu cầu là trách nhiệm của:

- ❖ Đơn vị vận hành hệ thống thông tin phải báo cáo chủ quản hệ thống thông tin hoặc cơ quan quản lý nhà nước chuyên ngành có thẩm quyền (Bộ Thông tin và Truyền thông);
- ❖ Chủ quản hệ thống thông tin tổng hợp, báo cáo Bộ Thông tin và Truyền thông.

2. Từ năm 2024, Bộ Thông tin và Truyền thông, các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ và Ủy ban nhân dân cấp tỉnh sẽ thống nhất triển khai chế độ báo cáo trong lĩnh vực bảo đảm an toàn hệ thống thông tin theo cấp độ thông qua Nền tảng hỗ trợ quản lý bảo đảm an toàn hệ thống thông tin theo cấp độ do Bộ Thông tin và Truyền thông (Cục An toàn thông tin) chủ trì triển khai miễn phí.