BAN CHẤP HÀNH TRUNG ƯƠNG
VĂN PHÒNG
*
Số 26-HD/VPTW

ĐẢNG CỘNG SẢN VIỆT NAM

Hà Nội, ngày 24 tháng 9 năm 2024

HƯỚNG DẪN
xác định, phê duyệt cấp độ an toàn hệ thống thông tin của cơ quan đảng

---

- Căn cứ Luật An toàn thông tin mạng năm 2015;

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

- Căn cứ 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;

- Căn cứ Chỉ thị số 41-CT/TW, ngày 24/3/2020 của Ban Bí thư về tăng cường phối hợp và triển khai đồng bộ các biện pháp bảo đảm an toàn, an ninh mạng;

- Căn cứ Quyết định số 27-QĐ/TW, ngày 10/8/2021 của Ban Bí thư về Chương trình ứng dụng công nghệ thông tin trong hoạt động của các cơ quan đảng giai đoạn 2021 - 2025;

- Xét đề nghị của Giám đốc Trung tâm Công nghệ thông tin - Cơ yếu,

Văn phòng Trung ương Đảng ban hành hướng dẫn xác định, phê duyệt cấp độ an toàn hệ thống thông tin của cơ quan đảng, cụ thể như sau:

I- MỤC ĐÍCH, YÊU CẦU, PHẠM VI

1. Mục đích

Hướng dẫn các cơ quan đảng từ Trung ương đến địa phương xác định cấp độ an toàn hệ thống thông tin và phê duyệt cấp độ an toàn hệ thống thông tin đối với các hệ thống thông tin thuộc phạm vi quản lý, tuân thủ và phù hợp với các quy định tại Nghị định số 85/2016/NĐ-CP, ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ (sau đây gọi tắt là Nghị định số 85/2016/NĐ-CP) và 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 01/7/2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ (sau đây gọi tắt là Thông tư số 12/2022/TT-BTTTT). Từ đó, là cơ sở để triển khai đầy đủ các phương án bảo đảm an toàn thông tin

(bao gồm các biện pháp quản lý và kỹ thuật) nhằm bảo vệ hệ thống thông tin phù hợp theo cấp độ đối với các hệ thống thông tin của các cơ quan đảng.

2. Yêu cầu

Tất cả các hệ thống thông tin đều phải được xác định cấp độ an toàn hệ thống thông tin. Việc đề xuất, thẩm định, phê duyệt phải được thực hiện theo đúng quy định hiện hành. Các cơ quan phải xác định chính xác các chủ thể tham gia vào quá trình xác định cấp độ an toàn hệ thống thông tin.

3. Phạm vi điều chỉnh

Văn bản này hướng dẫn xác định các chủ thể tham gia vào quá trình xác định cấp độ an toàn hệ thống thông tin; thẩm quyền, trình tự tổ chức thẩm định hồ sơ đề xuất cấp độ, phê duyệt cấp độ an toàn hệ thống thông tin đối với hệ thống thông tin do các cơ quan đảng chủ trì xây dựng, thuê dịch vụ, vận hành.

Các hệ thống thông tin dùng chung sẽ do cơ quan chủ trì xây dựng thực hiện xác định cấp độ an toàn hệ thống thông tin, các cơ quan nhận chuyển giao không phải thực hiện lại.

Các nội dung khác liên quan đến bảo đảm an toàn hệ thống thông tin theo cấp độ, chế độ báo cáo thực hiện theo Nghị định số 85/2016/NĐ-CP và Thông tư số 12/2022/TT-BTTTT.

II- XÁC ĐỊNH CẤP ĐỘ, ĐỀ XUẤT, THẨM ĐỊNH VÀ PHÊ DUYỆT

1. Chủ quản hệ thống thông tin

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, cụ thể:

- Đối với các hệ thống thông tin thuộc phạm vi quản lý hoặc do các cơ quan đảng tại Trung ương đầu tư xây dựng mới, nâng cấp hoặc mở rộng, thuê dịch vụ: Chủ quản hệ thống thông tin được xác định là Văn phòng Trung ương Đảng hoặc các cơ quan của Đảng ở Trung ương.

- Đối với các hệ thống thông tin do các cơ quan đảng ở địa phương đầu tư xây dựng mới, nâng cấp hoặc mở rộng, thuê dịch vụ:

+ Chủ quản hệ thống thông tin ở cấp tỉnh được xác định là ban thường vụ tỉnh uỷ, thành uỷ.

+ Chủ quản hệ thống thông tin ở cấp huyện được xác định là ban thường vụ huyện uỷ, quận uỷ.

+ Chủ quản hệ thống thông tin ở cấp xã được xác định là ban thường vụ huyện uỷ, quận uỷ.

- Trường hợp ban thường vụ huyện uỷ, quận uỷ không đủ năng lực làm chủ quản hệ thống thông tin (không đủ năng lực thực thi quy định tại Khoản 1, Khoản 2, Điều 20 Nghị định số 85/2016/NĐ-CP) thì cần báo cáo ban thường vụ tỉnh uỷ, thành uỷ và đề nghị ban thường vụ tỉnh uỷ, thành uỷ làm chủ quản hệ thống thông tin.

- Trong trường hợp cần thiết, chủ quản hệ thống thông tin uỷ quyền cho một tổ chức trực thuộc có đủ năng lực thực hiện trách nhiệm của chủ quản hệ thống thông tin quy định tại Khoản 2, Điều 20 Nghị định số 85/2016/NĐ-CP. Việc uỷ quyền trách nhiệm chủ quản hệ thống thông tin phải được thực hiện bằng văn bản, trong đó nêu rõ phạm vi của hệ thống, trách nhiệm tổ chức được uỷ quyền và thời hạn được uỷ quyền.

2. Đơn vị vận hành hệ thống thông tin

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

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

- 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 hoặc đơn vị chủ trì thuê dịch vụ công nghệ thông tin được xác định là đơn vị vận hành hệ thống thông tin. Trong giai đoạn vận hành cho đến khi kết thúc vận hành, khai thác, thanh lý, huỷ bỏ hệ thống thông tin, chủ đầu tư hoặc đơn vị chủ trì thuê dịch vụ công nghệ thông tin 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.

3. Đơn vị chuyên trách về công nghệ thông tin

Đơn vị chuyên trách công nghệ thông tin của chủ quản hệ thống thông tin được xác định như sau:

- Đối với các cơ quan đảng ở Trung ương là đơn vị trực thuộc được giao phụ trách về công nghệ thông tin.

- Đối với các cơ quan thuộc đảng bộ tỉnh là văn phòng tỉnh uỷ, thành uỷ.

- Đối với các cơ quan thuộc đảng bộ huyện là văn phòng huyện uỷ, quận uỷ.

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

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

Trong trường hợp 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 thì đơn vị chuyên trách về công nghệ thông tin làm nhiệm vụ đơn vị chuyên trách về an toàn thông tin. Chủ quản hệ thống thông tin giao thực hiện nhiệm vụ đơn vị chuyên trách về an toàn thông tin bằng văn bản cụ thể.

5. Nguyên tắc bảo đảm an toàn hệ thống thông tin theo cấp độ

- 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 huỷ 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.

6. Nguyên tắc xác định cấp độ

- Một hệ thống thông tin chỉ có một chủ quản hệ thống thông tin.

- 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.

7. Tiêu chí xác định cấp độ

Tiêu chí xác định cấp độ được thực hiện theo quy định tại Chương II của Nghị định số 85/2016/NĐ-CP. Cụ thể:

a) Tiêu chí xác định cấp độ 1

Hệ thống thông tin cấp độ 1 là hệ thống thông tin phục vụ hoạt động nội bộ của cơ quan, tổ chức và chỉ xử lý thông tin công cộng.

b) Tiêu chí xác định cấp độ 2

Hệ thống thông tin cấp độ 2 là hệ thống thông tin có một trong các tiêu chí cụ thể như sau:

- 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.

- Hệ thống thông tin phục vụ cán bộ, đảng viên và người dân, tổ chức thuộc một trong các loại hình như sau:

+ Cung cấp thông tin và dịch vụ trực tuyến từ mức độ 2 trở xuống theo quy định của pháp luật.

+ Cung cấp dịch vụ trực tuyến khác có xử lý thông tin riêng, thông tin cá nhân của dưới 5.000 người sử dụng.

- Hệ thống cơ sở hạ tầng thông tin phục vụ hoạt động của một cơ quan, tổ chức.

c) Tiêu chí xác định cấp độ 3

Hệ thống thông tin cấp độ 3 là hệ thống thông tin có một trong các tiêu chí cụ thể như sau:

- 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.

- Hệ thống thông tin phục vụ cán bộ, đảng viên và Nhân dân, tổ chức thuộc một trong các loại hình như sau:

+ Cung cấp thông tin và dịch vụ trực tuyến từ mức độ 3 trở lên theo quy định của pháp luật.

+ Cung cấp dịch vụ trực tuyến khác có xử lý thông tin riêng, thông tin cá nhân của từ 5.000 người sử dụng trở lên.

- 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 hoặc một số tỉnh.

d) Tiêu chí xác định cấp độ 4

Hệ thống thông tin cấp độ 4 là hệ thống thông tin có một trong các tiêu chí cụ thể như sau:

- 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.

- 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.

- 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.

đ) Tiêu chí xác định cấp độ 5

Hệ thống thông tin cấp độ 5 là hệ thống thông tin có một trong các tiêu chí cụ thể như sau:

- 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.

- 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.

- Hệ thống cơ sở hạ tầng thông tin quốc gia phục vụ kết nối liên thông hoạt động của Việt Nam với quốc tế.

- Hệ thống thông tin khác theo quyết định của Thủ tướng Chính phủ.

8. Thẩm quyền thẩm định và phê duyệt cấp độ

Thực hiện theo quy định tại Điều 12 Nghị định số 85/2016/NĐ-CP, cụ thể:

a) Đối với hệ thống thông tin được đề xuất là 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 và báo cáo chủ quản hệ thống thông tin.

b) Đối với hệ thống thông tin được đề xuất là cấp độ 3

- 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.

- Chủ quản hệ thống thông tin phê duyệt hồ sơ đề xuất cấp độ.

Hình thức tổ chức thẩm định đối với hệ thống thông tin được đề xuất là cấp độ 1, 2 và 3:

- Trường hợp đơn vị chuyên trách về an toàn thông tin đồng thời được chủ quản hệ thống thông tin giao là đơn vị vận hành hệ thống thông tin: Đơn vị chuyên trách về an toàn thông tin trình chủ quản hệ thống thông tin thành lập hội đồng thẩm định độc lập thực hiện nhiệm vụ thẩm định hồ sơ đề xuất cấp độ.

- Đối với hội đồng thẩm định độc lập do chủ quản hệ thống thông tin thành lập, chủ tịch hội đồng là lãnh đạo đơn vị chuyên trách về an toàn thông tin phụ trách về an toàn thông tin hoặc mời 1 chuyên gia uy tín trong lĩnh vực an toàn thông tin hoặc lãnh đạo sở thông tin và truyền thông tại địa phương (phụ trách an toàn thông tin) làm chủ tịch hội đồng.

- 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 có chuyên môn về an toàn thông tin tại các bộ, ngành hoặc sở thông tin và truyền thông, 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).

- 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.

c) Đối với hệ thống thông tin được đề xuất là cấp độ 4 hoặc cấp độ 5

- 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.

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

9. Trình tự, thủ tục xác định cấp độ đối với dự án đầu tư xây dựng mới hoặc mở rộng, nâng cấp hệ thống thông tin

Ngay sau khi được cấp có thẩm quyền phê duyệt chủ trương xây dựng mới hoặc nâng cấp mở rộng, thuê dịch vụ hệ thống thông tin. Chủ đầu tư/đơn vị chủ trì thuê dịch vụ tiến hành xây dựng tài liệu thiết kế hệ thống thông tin, là 1 trong các tài liệu báo cáo kinh tế - kỹ thuật (trong trường hợp dự án đầu tư áp dụng

phương án thiết kế 1 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 2 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):

- 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.

- Gửi hồ sơ đề xuất cấp độ cho cơ quan có thẩm quyền tổ chức thẩm định hồ sơ đề xuất cấp độ, phê duyệt cấp độ an toàn hệ thống thông tin.

10. Trình tự, thủ tục xác định, phê duyệt cấp độ đối với hệ thống thông tin đang vận hành

Căn cứ quy định tại Điều 14 Nghị định số 85/2016/NĐ-CP:

a) Lập hồ sơ đề xuất cấp độ

- Đơn vị vận hành hệ thống thông tin lập hồ sơ đề xuất cấp độ.

- Đối với hệ thống thông tin được đề xuất là cấp độ 1 hoặc cấp độ 2: Đơn vị vận hành hệ thống thông tin gửi hồ sơ đề xuất cấp độ tới đơn vị chuyên trách về an toàn thông tin để thẩm định, phê duyệt.

- Đối với hệ thống thông tin được đề xuất là cấp độ 3: Đơn vị vận hành hệ thống thông tin gửi hồ sơ đề xuất cấp độ tới đơn vị chuyên trách về an toàn thông tin thực hiện thẩm định.

- Đối với hệ thống thông tin được đề xuất là cấp độ 4 hoặc cấp độ 5:

+ Đơn vị vận hành hệ thống thông tin gửi hồ sơ đề xuất cấp độ tới đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin để xin ý kiến chuyên môn về sự phù hợp của đề xuất cấp độ và phương án bảo đảm an toàn hệ thống thông tin theo cấp độ.

+ Đơn vị vận hành hệ thống thông tin trình chủ quản hệ thống thông tin hồ sơ đề xuất cấp độ gửi tới cơ quan thẩm định Bộ Thông tin và Truyền thông.

b) Thẩm định hồ sơ đề xuất cấp độ

Cơ quan có thẩm quyền thực hiện thẩm định hồ sơ đề xuất cấp độ theo nội dung Mục 13, Phần II Hướng dẫn này.

c) Phê duyệt đề xuất cấp độ

- Đối với hệ thống thông tin được đề xuất là cấp độ 1 hoặc cấp độ 2:

Đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin phê duyệt đề xuất cấp độ, gửi báo cáo chủ quản hệ thống thông tin.

- Đối với hệ thống thông tin được đề xuất là cấp độ 3 hoặc cấp độ 4: Chủ quản hệ thống thông tin phê duyệt hồ sơ đề xuất cấp độ.

Đơn vị vận hành hệ thống thông tin trình chủ quản hệ thống thông tin phê duyệt đề xuất cấp độ.

- 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.

+ Đơn vị vận hành hệ thống thông tin trình chủ quản hệ thống thông tin phê duyệt phương án bảo đảm an toàn thông tin.

11. Trình tự, thủ tục xác định lại cấp độ đối với hệ thống thông tin đã được phê duyệt cấp độ

Căn cứ quy định tại Điều 18 Nghị định số 85/2016/NĐ-CP:

Đối với hệ thống thông tin đã được phê duyệt cấp độ, trong trường hợp phải xác định lại cấp độ cho phù hợp với tình hình thực tế thì thực hiện theo trình tự, thủ tục xác định lần đầu.

12. Hồ sơ đề xuất cấp độ

Căn cứ quy định tại Điều 15 Nghị định số 85/2016/NĐ-CP và Điều 8 Thông tư số 12/2022/TT-BTTTT:

Hồ sơ đề xuất cấp độ, bao gồm các thành phần sau đây:

- 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.

- Ý kiến về mặt chuyên môn của đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin đối với hệ thống thông tin đề xuất cấp độ 4 hoặc cấp độ 5.

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

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

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

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

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

b) Thuyết minh về việc đề xuất cấp độ, bao gồm các nội dung:

- Danh mục các hệ thống thông tin và cấp độ tương ứng, bao gồm: Tên hệ thống thông tin, cấp độ đề xuất, căn cứ đề xuất đối với từng hệ thống thông tin.

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

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

+ 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.

+ 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.

+ 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.

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

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

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

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

Nội dung thuyết minh chi tiết thực hiện theo Điều 10, Thông tư số 12/2022/TT-BTTTT.

(Chi tiết mẫu Hồ sơ đề xuất cấp độ tại Phụ lục 2).

13. Thẩm định hồ sơ đề xuất cấp độ

Căn cứ quy định tại Điều 16, Nghị định số 85/2016/NĐ-CP, nội dung thẩm định hồ sơ đề xuất cấp độ:

- Sự phù hợp về việc đề xuất cấp độ.

- 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.

- 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.

14. Hồ sơ phê duyệt đề xuất cấp độ

Căn cứ quy định tại Điều 17, Nghị định số 85/2016/NĐ-CP, hồ sơ phê duyệt đề xuất cấp độ bao gồm:

- Hồ sơ đề xuất cấp độ.

- Ý kiến thẩm định của cơ quan chủ trì thẩm định đối với hệ thống thông tin đề xuất từ cấp độ 3 trở lên.

15. Thời điểm phê duyệt hồ sơ đề xuất cấp độ

Căn cứ các quy định tại Khoản 6, Điều 9 và Điều 15, Thông tư số 12/2022/TT-BTTTT:

- Hồ sơ đề xuất cấp độ an toàn thông tin của hệ thống thông tin được đầu tư xây dựng mới, nâng cấp hoặc mở rộng, thuê dịch vụ phải được phê duyệt trước khi đưa hệ thống thông tin vào vận hành, khai thác.

- 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 tương ứng.

16. Hệ thống thông tin đang vận hành, khai thác chưa được phê duyệt Hồ sơ đề xuất cấp độ

Căn cứ quy định tại Điều 14, Nghị định số 85/2016/NĐ-CP, đối với các hệ thống thông tin đang vận hành, khai thác nhưng chưa được phê duyệt cấp độ an toàn hệ thống thông tin, đơn vị vận hành hệ thống thông tin có trách nhiệm hoàn thành việc xây dựng hồ sơ đề xuất cấp độ gửi cơ quan có thẩm quyền tổ chức thẩm định hồ sơ đề xuất cấp độ, phê duyệt cấp độ an toàn hệ thống thông tin.

III- TỔ CHỨC THỰC HIỆN

Các cơ quan đảng ở Trung ương, các cơ quan đảng ở địa phương tổ chức triển khai thực hiện Hướng dẫn này.

Trong quá trình triển khai thực hiện, nếu có khó khăn, vướng mắc, đề nghị các cơ quan trao đổi trực tiếp với Văn phòng Trung ương Đảng (qua Trung tâm Công nghệ thông tin - Cơ yếu) để kịp thời phối hợp, giải quyết.

Nơi nhận:
- Các cơ quan đảng ở Trung ương,
- Các tỉnh uỷ, thành uỷ,
- Trung tâm Công nghệ thông tin - Cơ yếu,
- Lưu Văn phòng Trung ương Đảng.

K/T CHÁNH VĂN PHÒNG
PHÓ CHÁNH VĂN PHÒNG

ĐẢNG CỘNG SẢN VIỆT NAM
VĂN PHÒNG
BAN CHẤP HÀNH TRUNG ƯƠNG

Ký bởi: VĂN PHÒNG TRUNG ƯƠNG ĐẢNG
Email: vanphongtrunguongdang@vptw.dcs.vn
Cơ quan: VĂN PHÒNG TRUNG ƯƠNG ĐẢNG
Ngày ký: 2024-09-27 08:18:03 +07:00

Bùi Văn Thạch

PHỤ LỤC 1
MẪU VĂN BẢN XÁC ĐỊNH CẤP ĐỘ AN TOÀN HỆ THỐNG THÔNG TIN

(Kèm theo Hướng dẫn số 26-HD/VPTW, ngày 24/9/2024 của Văn phòng Trung ương Đảng)

Mẫu số 01	Văn bản đề nghị thẩm định, phê duyệt hồ sơ đề xuất cấp độ
Mẫu số 02	Văn bản đề nghị thẩm định hồ sơ đề xuất cấp độ
Mẫu số 03	Văn bản xin ý kiến chuyên môn về hồ sơ đề xuất cấp độ (cấp độ 4,5)
Mẫu số 04	Ý kiến thẩm định hồ sơ đề xuất cấp độ
Mẫu số 05	Tờ trình phê duyệt hồ sơ đề xuất cấp độ
Mẫu số 06	Quyết định phê duyệt cấp độ an toàn hệ thống thông tin
Mẫu số 07	Quyết định phê duyệt phương án bảo đảm an toàn thông tin

Mẫu số 01

TÊN CƠ QUAN, TỔ CHỨC CẤP TRÊN **TÊN CƠ QUAN, TỔ CHỨC** * Số ….-….. *V/v đề nghị thẩm định, phê duyệt hồ sơ đề xuất cấp độ*	**ĐẢNG CỘNG SẢN VIỆT NAM** *….., ngày…..tháng…..năm…..*

Kính gửi: (Đơn vị chuyên trách về an toàn thông tin),

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

(Căn cứ các văn bản hướng dẫn thi hành Luật An toàn thông tin mạng và các văn bản liên quan);

(Tên cơ quan, tổ chức) đề nghị thẩm định, phê duyệt hồ sơ đề xuất cấp độ với các nội dung sau:

Phần 1. Thông tin chung

1. Tên hệ thống thông tin.

2. Đơn vị vận hành hệ thống thông tin.

3. Địa chỉ.

4. Cấp độ an toàn hệ thống thông tin đề xuất.

Phần 2. Hồ sơ kèm theo

1. Tài liệu mô tả, thuyết minh tổng quan về hệ thống thông tin.

2. Tài liệu thiết kế thi công đã được cấp có thẩm quyền phê duyệt hoặc tài liệu có giá trị tương đương.

3. Tài liệu thuyết minh về việc đề xuất cấp độ căn cứ trên các tiêu chí theo quy định của pháp luật.

4. Tài liệu thuyết minh phương án bảo đảm an toàn thông tin theo cấp độ tương ứng.

(Tên cơ quan, tổ chức) đề nghị (Đơn vị chuyên trách về an toàn thông tin) thẩm định và phê duyệt hồ sơ đề xuất cấp độ của hệ thống thông tin (Tên hệ thống thông tin).

Nơi nhận: - Như trên, - ….	**QUYỀN HẠN, CHỨC VỤ CỦA NGƯỜI KÝ** (chữ ký, dấu) **Họ và tên**

Mẫu số 02

TÊN CƠ QUAN, TỔ CHỨC CẤP TRÊN **TÊN CƠ QUAN, TỔ CHỨC** * Số ….-….. *V/v đề nghị thẩm định hồ sơ đề xuất cấp độ*	**ĐẢNG CỘNG SẢN VIỆT NAM** *….., ngày…..tháng…..năm…..*

Kính gửi: (Đơn vị chuyên trách về an toàn thông tin),

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

(Căn cứ các văn bản hướng dẫn thi hành Luật An toàn thông tin mạng và các văn bản liên quan);

(Tên cơ quan, tổ chức) đề nghị (Cơ quan thẩm định) thẩm định hồ sơ đề xuất cấp độ với các nội dung sau:

Phần 1. Thông tin chung

1. Tên hệ thống thông tin.

2. Đơn vị vận hành hệ thống thông tin.

3. Địa chỉ.

4. Cấp độ an toàn hệ thống thông tin đề xuất.

Phần 2. Hồ sơ kèm theo

1. Tài liệu mô tả, thuyết minh tổng quan về hệ thống thông tin.

2. Tài liệu thiết kế thi công đã được cấp có thẩm quyền phê duyệt hoặc tài liệu có giá trị tương đương.

3. Tài liệu thuyết minh về việc đề xuất cấp độ căn cứ trên các tiêu chí theo quy định của pháp luật.

4. Tài liệu thuyết minh phương án bảo đảm an toàn thông tin theo cấp độ tương ứng.

5. Ý kiến về mặt chuyên môn của đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin (đối với hệ thống thông tin đề xuất cấp độ 4 hoặc cấp độ 5).

(Tên cơ quan, tổ chức) đề nghị (Cơ quan thẩm định) cho ý kiến thẩm định hồ sơ đề xuất cấp độ an toàn hệ thống thông tin đối với (Tên hệ thống thông tin).

Nơi nhận: - Như trên, - ….	**QUYỀN HẠN, CHỨC VỤ CỦA NGƯỜI KÝ** (chữ ký, dấu) **Họ và tên**

Mẫu số 03

TÊN CƠ QUAN, TỔ CHỨC CẤP TRÊN **TÊN CƠ QUAN, TỔ CHỨC** * Số ….-….. *V/v xin ý kiến chuyên môn về hồ sơ đề xuất cấp độ*	**ĐẢNG CỘNG SẢN VIỆT NAM** *….., ngày…..tháng…..năm…..*

Kính gửi: (Đơn vị chuyên trách về an toàn thông tin),

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

(Căn cứ các văn bản hướng dẫn thi hành Luật An toàn thông tin mạng và các văn bản liên quan);

(Tên cơ quan, tổ chức) đề nghị (Đơn vị chuyên trách về an toàn thông tin) cho ý kiến chuyên môn về hồ sơ đề xuất cấp độ với các nội dung sau:

Phần 1. Thông tin chung

1. Tên hệ thống thông tin.

2. Đơn vị vận hành hệ thống thông tin.

3. Địa chỉ.

4. Cấp độ an toàn hệ thống thông tin đề xuất.

Phần 2. Hồ sơ kèm theo

1. Tài liệu mô tả, thuyết minh tổng quan về hệ thống thông tin.

2. Tài liệu thiết kế thi công đã được cấp có thẩm quyền phê duyệt hoặc tài liệu có giá trị tương đương.

3. Tài liệu thuyết minh về việc đề xuất cấp độ căn cứ trên các tiêu chí theo quy định của pháp luật.

4. Tài liệu thuyết minh phương án bảo đảm an toàn thông tin theo cấp độ tương ứng.

(Tên cơ quan, tổ chức) đề nghị (Đơn vị chuyên trách về an toàn thông tin) cho ý kiến về sự phù hợp của đề xuất cấp độ và phương án bảo đảm an toàn hệ thống thông tin theo cấp độ của hệ thống thông tin (Tên hệ thống thông tin).

Nơi nhận: - Như trên, - ….	**QUYỀN HẠN, CHỨC VỤ CỦA NGƯỜI KÝ** (chữ ký, dấu) **Họ và tên**

Mẫu số 04

TÊN CƠ QUAN, TỔ CHỨC CẤP TRÊN **TÊN CƠ QUAN, TỔ CHỨC** * Số ….-….. *V/v ý kiến thẩm định hồ sơ đề xuất cấp độ*	**ĐẢNG CỘNG SẢN VIỆT NAM** *….., ngày…..tháng…..năm…..*

Kính gửi: (Chủ quản hệ thống thông tin/Đơn vị vận hành hệ thống thông tin/Đơn vị chuyên trách về an toàn thông tin).

(Tên cơ quan thẩm định) nhận được Công văn số ….. ngày ….. tháng..... năm ….. của (Tên cơ quan đề nghị) về việc thẩm định hồ sơ đề xuất cấp độ của hệ thống thông tin đối với (Tên hệ thống thông tin). Sau khi xem xét, tổng hợp ý kiến và kết quả thẩm định của các cơ quan, tổ chức có liên quan (Tên cơ quan thẩm định) có ý kiến thẩm định như sau:

Phần 1. Hồ sơ, tài liệu thẩm định

1. Tài liệu mô tả, thuyết minh tổng quan về hệ thống thông tin.

2. Tài liệu thiết kế thi công đã được cấp có thẩm quyền phê duyệt hoặc tài liệu có giá trị tương đương.

3. Tài liệu thuyết minh về việc đề xuất cấp độ căn cứ trên các tiêu chí theo quy định của pháp luật.

4. Tài liệu thuyết minh phương án bảo đảm an toàn thông tin theo cấp độ tương ứng.

5. Ý kiến về mặt chuyên môn của đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin đối với hệ thống thông tin đề xuất cấp độ 4 hoặc cấp độ 5.

Phần 2. Căn cứ pháp lý để thẩm định

1. Căn cứ Luật An toàn thông tin mạng ngày 19/11/2015.

2. Căn cứ các văn bản hướng dẫn thi hành Luật An toàn thông tin mạng.

3. Các căn cứ pháp lý khác có liên quan.

Phần 3. Tổ chức thẩm định

1. Đơn vị chủ trì thẩm định.

2. Đơn vị phối hợp thẩm định.

3. Hình thức thẩm định: Tổ chức họp hoặc lấy ý kiến bằng văn bản hoặc áp dụng cả hai hình thức (nếu cần thiết).

Phần 4. Ý kiến thẩm định

1. Tổng hợp ý kiến thẩm định của đơn vị phối hợp theo quy định tại Khoản 3, Điều 12, Nghị định số 85/2016/NĐ-CP.

2. Ý kiến thẩm định về sự phù hợp về việc đề xuất cấp độ theo quy định tại Điều 16, Nghị định số 85/2016/NĐ-CP.

3. Ý kiến khác (nếu có).

Phần 5. Kết luận

Hồ sơ đề xuất cấp độ hệ thống thông tin là phù hợp/chưa phù hợp (nếu chưa phù hợp đề nghị chỉ rõ những nội dung chưa phù hợp) để theo cấp độ đề xuất.

Trên đây là ý kiến thẩm định của (Cơ quan thẩm định) cho hồ sơ đề xuất cấp độ của hệ thống thông tin (Tên hệ thống thông tin). Đề nghị cơ quan (Tên cơ quan đề nghị) xem xét báo cáo cấp có thẩm quyền điều chỉnh (nếu yêu cầu điều chỉnh) hoặc trình cơ quan có thẩm quyền phê duyệt (nếu chấp thuận đề xuất của cơ quan trình).

Nơi nhận:
- Như trên,
- ….

QUYỀN HẠN, CHỨC VỤ CỦA NGƯỜI KÝ

(chữ ký, dấu)[1]

Họ và tên

[1] Trong trường hợp văn bản của Hội đồng thẩm định chỉ cần chữ ký của Chủ tịch Hội đồng.

Mẫu số 05

TÊN CƠ QUAN, TỔ CHỨC CẤP TRÊN **TÊN CƠ QUAN, TỔ CHỨC** * Số ….-…..	**ĐẢNG CỘNG SẢN VIỆT NAM** *….., ngày…..tháng…..năm…..*

TỜ TRÌNH
về việc phê duyệt đề xuất cấp độ

Kính gửi: (Cơ quan liên quan có thẩm quyền),

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

(Căn cứ các văn bản hướng dẫn thi hành Luật An toàn thông tin mạng và các văn bản liên quan);

Căn cứ ý kiến thẩm định của đơn vị chuyên trách về công nghệ thông tin/cơ quan thẩm định;

(Tên cơ quan, tổ chức) trình phê duyệt hồ sơ đề xuất cấp độ với các nội dung sau:

Phần 1. Thông tin chung

1. Tên hệ thống thông tin.

2. Đơn vị vận hành hệ thống thông tin.

3. Địa chỉ.

4. Cấp độ an toàn hệ thống thông tin đề xuất.

Phần 2. Hồ sơ kèm theo

1. Tài liệu mô tả, thuyết minh tổng quan về hệ thống thông tin.

2. Tài liệu thiết kế thi công đã được cấp có thẩm quyền phê duyệt hoặc tài liệu có giá trị tương đương.

3. Tài liệu thuyết minh về việc đề xuất cấp độ căn cứ trên các tiêu chí theo quy định của pháp luật.

4. Tài liệu thuyết minh phương án bảo đảm an toàn thông tin theo cấp độ tương ứng.

5. Ý kiến về mặt chuyên môn của đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin đối với hệ thống thông tin đề xuất cấp độ 4 hoặc cấp độ 5.

6. Ý kiến thẩm định của cơ quan chủ trì thẩm định đối với hệ thống thông tin đề xuất từ cấp độ 3 trở lên.

(Tên cơ quan) trình (Chủ quản hệ thống thông tin) xem xét, quyết định phê duyệt đề xuất cấp độ của hệ thống thông tin (Tên hệ thống thông tin).

Nơi nhận:
- Như trên,
- ….

QUYỀN HẠN, CHỨC VỤ CỦA NGƯỜI KÝ

(chữ ký, dấu)

Họ và tên

Mẫu số 06

TÊN CƠ QUAN, TỔ CHỨC CẤP TRÊN **TÊN CƠ QUAN, TỔ CHỨC** *(là Chủ quản Hệ thống thông tin)* * Số ….-…..	**ĐẢNG CỘNG SẢN VIỆT NAM** *….., ngày…..tháng…..năm…..*

QUYẾT ĐỊNH
về việc phê duyệt cấp độ an toàn hệ thống thông tin

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

(Căn cứ các văn bản hướng dẫn thi hành Luật An toàn thông tin mạng và các văn bản liên quan);

Xét đề nghị của cơ quan (Tên đơn vị đề nghị),

THỦ TRƯỞNG CƠ QUAN, ĐƠN VỊ *(Ghi chức vụ của người đại diện)*
QUYẾT ĐỊNH

Điều 1. Phê duyệt cấp độ an toàn hệ thống thông tin đối với (Tên hệ thống thông tin) cụ thể như sau:

1. Thông tin chung

a) Tên hệ thống thông tin.

b) Đơn vị vận hành hệ thống thông tin.

c) Địa chỉ.

2. Cấp độ an toàn hệ thống thông tin: (cấp độ).

3. Phương án bảo đảm an toàn thông tin:

a) Phương án bảo đảm an toàn thông tin trong thiết kế hệ thống thông tin tương ứng với cấp độ (cấp độ) là phù hợp với tiêu chuẩn quốc gia (Tên tiêu chuẩn), quy chuẩn kỹ thuật quốc gia (Tên quy chuẩn) về bảo đảm an toàn hệ thống thông tin theo cấp độ.

b) Phương án bảo đảm an toàn thông tin trong quá trình vận hành hệ thống tương ứng với cấp độ (cấp độ) là phù hợp với tiêu chuẩn quốc gia (Tên tiêu chuẩn),

quy chuẩn kỹ thuật quốc gia (Tên quy chuẩn) về bảo đảm an toàn hệ thống thông tin theo cấp độ.

Điều 2. Tổ chức thực hiện

1. Cơ quan (Tên đơn vị đề nghị) chịu trách nhiệm:

a) Thực hiện trách nhiệm bảo đảm an toàn hệ thống thông tin mình quản lý theo các quy định tại Điều 22, Nghị định số 85/2016/NĐ-CP.

b) Các nội dung khác (nếu có).

2. Trách nhiệm của các cơ quan liên quan khác (nếu có).

Điều 3. Điều khoản thi hành

1. Cơ quan (Tên đơn vị đề xuất) và các cơ quan liên quan khác chịu trách nhiệm thi hành Quyết định này.

2. Đơn vị chuyên trách về an toàn thông tin chịu trách nhiệm kiểm tra, giám sát việc thực hiện Quyết định này báo cáo cơ quan (Chủ quản hệ thống thông tin) theo quy định của pháp luật.

Nơi nhận:
- Như trên,
- ….

QUYỀN HẠN, CHỨC VỤ CỦA NGƯỜI KÝ

(chữ ký, dấu)

Họ và tên

Mẫu số 07

TÊN CƠ QUAN, TỔ CHỨC CẤP TRÊN
TÊN CƠ QUAN, TỔ CHỨC
(là Chủ quản Hệ thống thông tin)
*
Số ….-…..

ĐẢNG CỘNG SẢN VIỆT NAM

….., ngày…..tháng…..năm…..

QUYẾT ĐỊNH
về việc phê duyệt phương án bảo đảm an toàn thông tin

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

(Căn cứ các văn bản hướng dẫn thi hành Luật An toàn thông tin mạng và các văn bản liên quan);

Xét đề nghị của cơ quan (Tên đơn vị đề nghị),

THỦ TRƯỞNG CƠ QUAN, ĐƠN VỊ *(Ghi chức vụ của người đại diện)*
QUYẾT ĐỊNH

Điều 1. Phê duyệt phương án bảo đảm an toàn thông tin đối với (Tên hệ thống thông tin) cụ thể như sau:

1. Thông tin chung

a) Tên hệ thống thông tin.

b) Đơn vị vận hành hệ thống thông tin.

c) Địa chỉ.

2. Phương án bảo đảm an toàn thông tin:

a) Phương án bảo đảm an toàn thông tin trong thiết kế hệ thống thông tin tương ứng với cấp độ (cấp độ) là phù hợp với tiêu chuẩn quốc gia (Tên tiêu chuẩn), quy chuẩn kỹ thuật quốc gia (Tên quy chuẩn) về bảo đảm an toàn hệ thống thông tin theo cấp độ.

b) Phương án bảo đảm an toàn thông tin trong quá trình vận hành hệ thống tương ứng với cấp độ (cấp độ) là phù hợp với tiêu chuẩn quốc gia (Tên tiêu chuẩn), quy chuẩn kỹ thuật quốc gia (Tên quy chuẩn) về bảo đảm an toàn hệ thống thông tin theo cấp độ.

Điều 2. Tổ chức thực hiện

1. Cơ quan (Tên đơn vị đề nghị) chịu trách nhiệm:

a) Thực hiện trách nhiệm bảo đảm an toàn hệ thống thông tin mình quản lý theo các quy định tại Điều 22, Nghị định số 85/2016/NĐ-CP.

b) Các nội dung khác (nếu có).

2. Trách nhiệm của các cơ quan liên quan khác (nếu có).

Điều 3. Điều khoản thi hành

1. Cơ quan (Tên đơn vị đề xuất) và các cơ quan liên quan khác chịu trách nhiệm thi hành Quyết định này.

2. Đơn vị chuyên trách về an toàn thông tin chịu trách nhiệm kiểm tra, giám sát việc thực hiện Quyết định này báo cáo cơ quan (Chủ quản hệ thống thông tin) theo quy định của pháp luật.

Nơi nhận:
- Như trên,
- ….

QUYỀN HẠN, CHỨC VỤ CỦA NGƯỜI KÝ

(chữ ký, dấu)

Họ và tên

PHỤ LỤC 2
MẪU HỒ SƠ ĐỀ XUẤT CẤP ĐỘ

(Kèm theo Hướng dẫn số 26-HD/VPTW, ngày 24/9/2024 của Văn phòng Trung ương Đảng)

---

1. 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:

1.1. 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 uỷ 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 uỷ quyền, đơn vị được uỷ quyền, phạm vi, thời gian uỷ quyền.

1.2. 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.

1.3. 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.

1.4. 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:

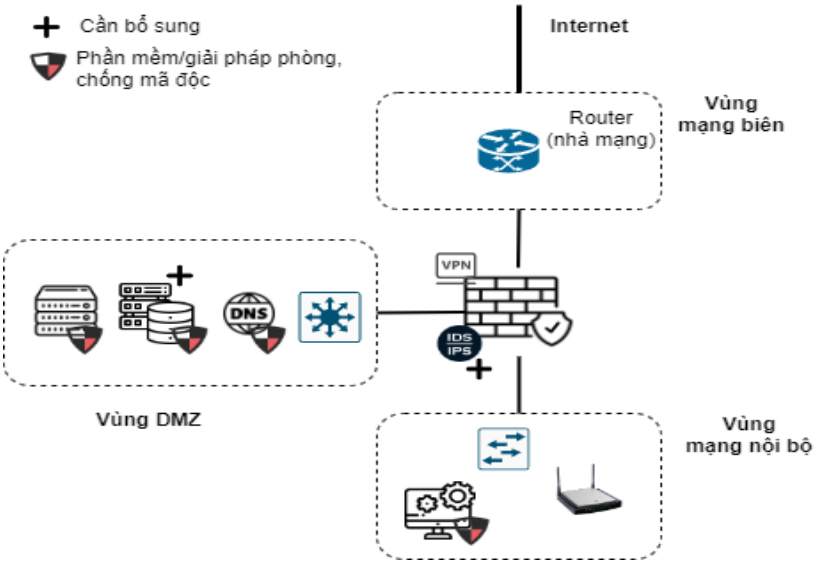
1.4.1. Mô hình lô-gic của hệ thống

Khái niệm: *Mô hình lô-gic của hệ thống thông tin*[2] 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 1. Mô hình lô-gic tham khảo:

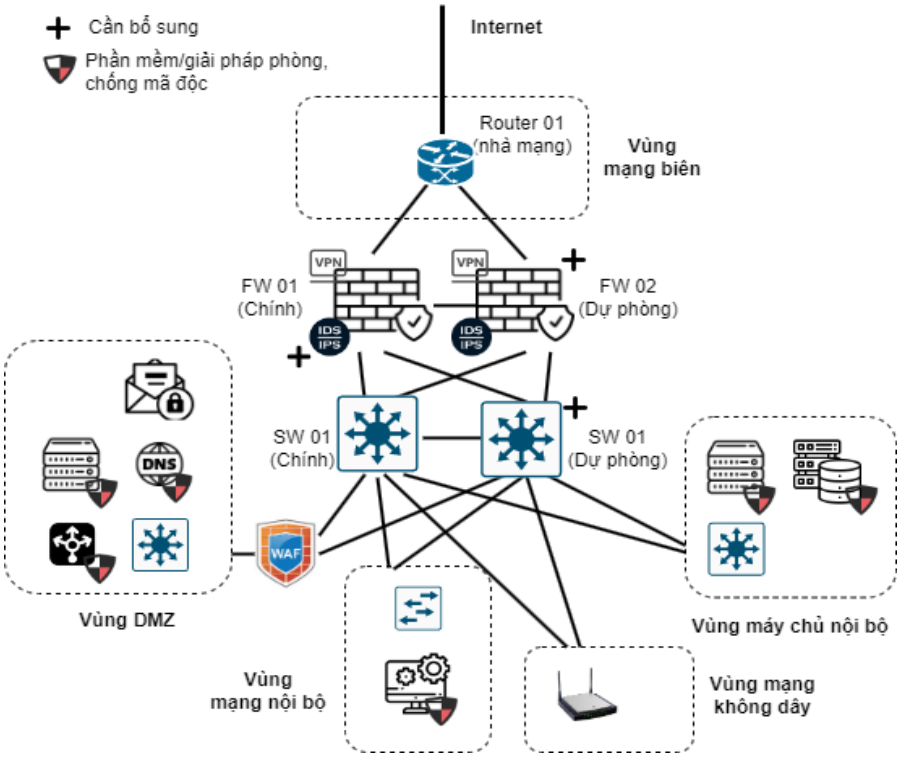
(i) Đối với hệ thống thông tin cấp độ 1:



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

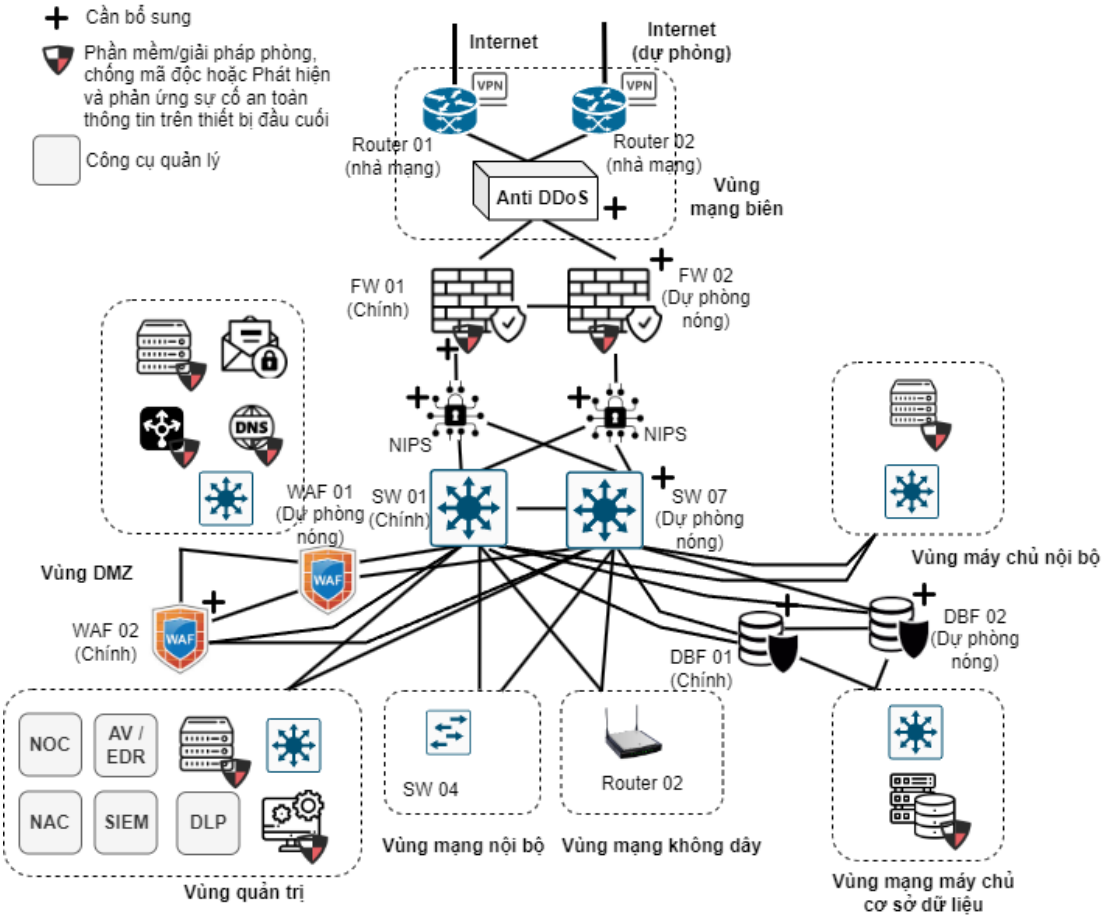
(ii) Đối với hệ thống thông tin cấp độ 2:

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



Hình 2. 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 3. Mô hình lô-gic tham khảo đối với hệ thống thông tin cấp độ 3

Lưu ý:

(1) Bên cạnh việc bảo đảm 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 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 1** ở trên. Đây chính là các thành phần được xác định phải sớm đầu tư bổ sung để bảo đảm 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.

Bảng 1: Danh sách các phân vùng mạng tối thiểu

STT	Vùng mạng[3]	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

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

STT	Vùng mạng[3]	Cấp độ				
		1	2	3	4	5
4	*Vùng máy chủ nội bộ* (internal server zone hay servers 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.		x	x	x	x
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 pháp 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

1.4.2. Mô hình vật lý của hệ thống

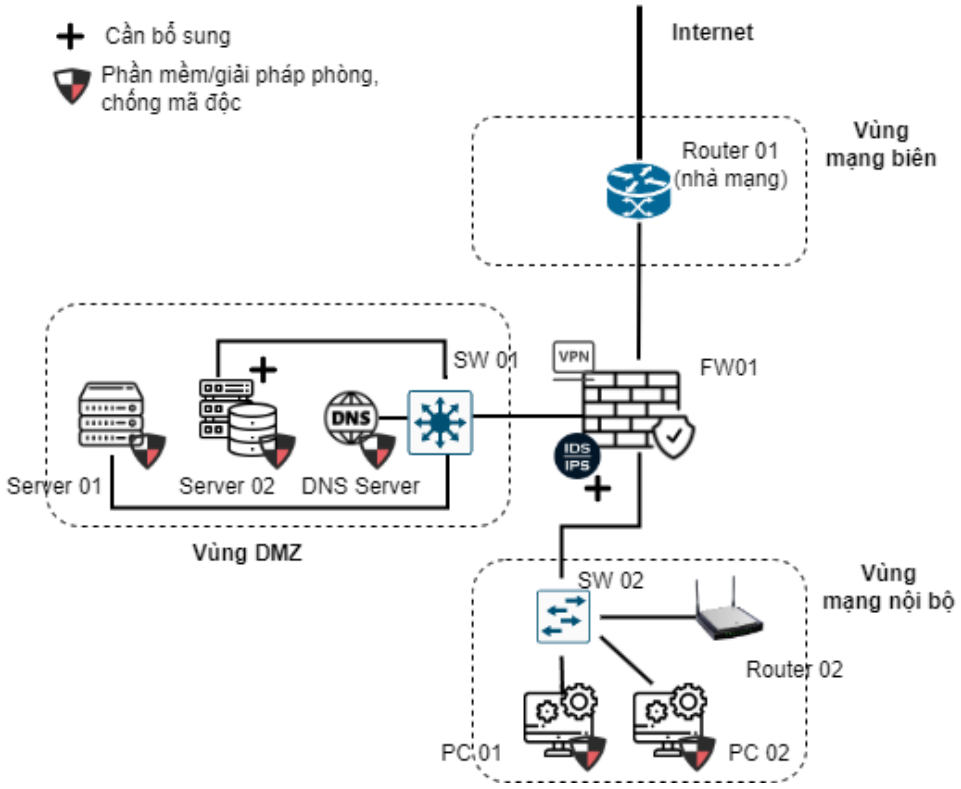
Khái niệm: *Mô hình vật lý của hệ thống thông tin*[4] là mô hình thể hiện mức chi tiết của mô hình lô-gic. Mô hình này biểu diễn thiết kế của hệ thống thông tin dựa trên mô hình lô-gic và giải pháp thiết kế của hệ thống đã được lựa chọn với các thông tin về giải pháp, thông số kỹ thuật và thiết bị, công 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 2. Mô hình vật lý tham khảo:

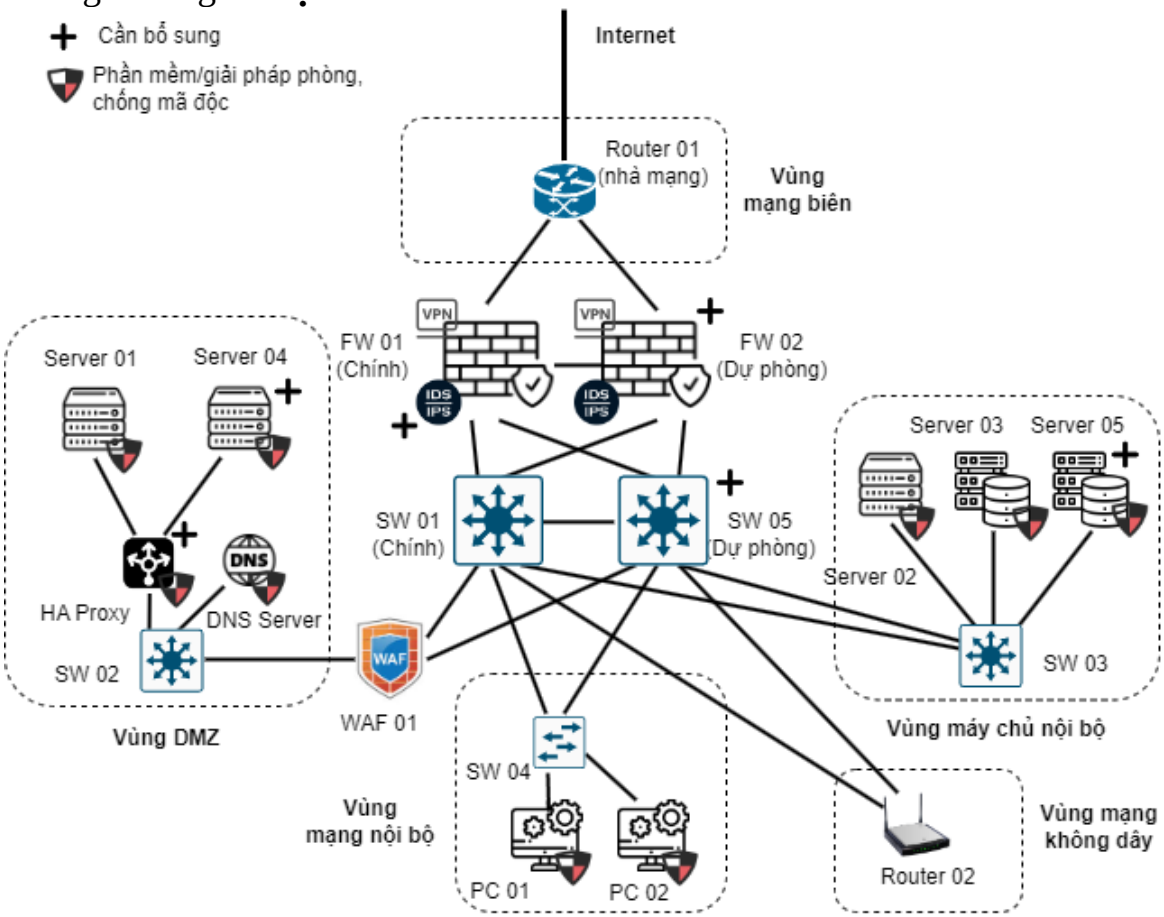
(i) Đối với hệ thống thông tin cấp độ 1: Mô hình này tương ứng với mô hình lô-gic trong **Ví dụ 1** ở trên.

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



Hình 4. 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 1** ở trên.



Hình 5. 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 lô-gic, mô hình vật lý của hệ thống thuộc tài liệu thiết kế hệ thống thông tin.

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

Bảng 1: Danh mục thiết bị trong hệ thống

STT	Tên thiết bị/chủng loại[5]	Vị trí triển khai[6]	Mục đích sử dụng
1	Firewall FW01[7] 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[8]	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.

[5] 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).
[6] Chỉ rõ vùng mạng phục vụ triển khai.
[7] Thông tin được thuyết minh trong Bảng 2, 3, 4 là **ví dụ minh hoạ** ứng với mô hình vật lý tại Hình 4.
[8] 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.

STT	Tên thiết bị/chủng loại[5]	Vị trí triển khai[6]	Mục đích sử dụng
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 xem là thiết bị mạng chính hay không để làm căn cứ đầu tư dự phòng cho phù hợp]*

Thiết bị mạng chính hoặc quan trọng[9] 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.

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

Bảng 2. Danh mục ứng dụng/dịch vụ cung cấp bởi hệ thống

STT	Tên ứng dụng/dịch vụ[10]	Máy chủ triển khai[11]	Vị trí triển khai[12]	Hệ điều hành máy chủ	Mục đích sử dụng[13]
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.
2	*[Ví dụ: Trang thông tin điện tử của Uỷ 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

[9] Khoản 2, Điều 3 Thông tư số 12/2022/TT-BTTTT.
[10] 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).
[11] 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.
[12] Chỉ rõ vùng mạng phục vụ triển khai.
[13] 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.

STT	Tên ứng dụng/dịch vụ[10]	Máy chủ triển khai[11]	Vị trí triển khai[12]	Hệ điều hành máy chủ	Mục đích sử dụng[13]
					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[14].
3	…	*[Các máy chủ khác nếu có]*	Vùng DMZ	…	…

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

Bảng 3. Quy hoạch các vùng mạng và địa chỉ IP trong hệ thống

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	//[15]

2. 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:

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

Bảng 4. 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 huyện uỷ 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	…	…	…

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

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.

2.2. 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 3. Thuyết minh chi tiết đề xuất cấp độ đối với Trang thông tin điện tử của huyện X:

Căn cứ phạm vi, quy mô và đối tượng phục vụ của hệ thống, Trang thông tin điện tử của huyện uỷ 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 huyện uỷ và các cơ quan chuyên môn, đơn vị trực thuộc huyện uỷ; 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 huyện uỷ 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 huyện uỷ X là hệ thống thông tin cấp độ 1.

2.3. Thuyết minh bổ sung đối với các hệ thống thông tin 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 đề xuất cấp độ 4 hoặc cấp độ 5, ngoài các nội dung phải thuyết minh tại các Mục 1.1 và 1.2 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.

3. 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 bảo đảm 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, tuỳ 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.

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

3.1.1. 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, huỷ bỏ*	x	x	x	x	x

Bảng 5. 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. 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][16].

- Quyết định số …/QĐ-… ngày …/…/… của [Tên đơn vị vận hành][17] 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)[18], các tài liệu khác...

(4) 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

[16] Quy chế chung (nếu có).
[17] 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.
[18] 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.

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 **3 tháng** kể từ ngày hệ thống thông tin được phê duyệt cấp độ an toàn thông tin.

3.1.2. 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 bảo đảm 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 3 năm (đối với cấp độ 1 và cấp độ 2), 2 năm (đối với cấp độ 3), hằng năm (đối với cấp độ 4), 6 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 bảo đảm an toàn thông tin cho hệ thống thông tin đã được cập nhật, điều chỉnh, bổ sung hoặc thay thế (nếu có).

3.1.3. 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).

3.1.4. 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 bảo đảm 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 hoá tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc.

3.1.5. 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 mô 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, 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, 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, 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).

3.1.6. 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.

3.1.7. 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.

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

Tương tự phương án quản lý rủi ro an toàn thông tin, phương án kết thúc vận hành, khai thác, thanh lý, huỷ 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, huỷ 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.

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

3.2.1. 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 6. 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 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 3 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.

3.2.2. 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 bảo đảm 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 chí 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 6. Đối với hệ thống thông tin cấp độ 1 có mô hình lô-gic được minh hoạ tại **Ví dụ 1** (Hình 1), mô hình vật lý được minh hoạ tại **Ví dụ 2** (Hình 4) và có danh sách thiết bị như tại **Bảng 2** 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][19] 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.
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.

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

STT	Yêu cầu	Hiện trạng	Mô tả phương án triển khai/Lý do không triển khai
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 **3 tháng** kể từ khi hệ thống thông tin được phê duyệt cấp độ an toàn thông tin[20].
3	Có phương án phòng, chống mã độc cho máy chủ và máy trạm sử dụng sản phẩm phòng, chống mã độc hoặc phương án tương đương	[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 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.

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

STT	Yêu cầu	Hiện trạng	Mô tả phương án triển khai/Lý do không triển khai
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[21] / Thiết bị[22]	Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên các thiết bị mạng chính
1	Firewall FW01	+
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[23].
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[24].

[21] Các tiêu chí cần thiết lập, cấu hình đáp ứng yêu cầu theo Tiêu chuẩn TCVN 11930: 2017.
[22] Các thiết bị mạng chính được xác định ở Bảng 2.
[23] Lưu ý: Sau khi được bổ sung, cần cập nhật lại phương án triển khai cho phù hợp.
[24] Lưu ý: Sau khi được bổ sung, cần cập nhật lại phương án triển khai cho phù hợp.

(vi) Bảo vệ thiết bị hệ thống:

STT	Yêu cầu / Thiết bị[25]	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	[…]	+	+

3.2.3. 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 3.2.2** 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 7. Đối với hệ thống thông tin cấp độ 1 có mô hình lô-gic được minh hoạ tại **Ví dụ 1** (Hình 1), mô hình vật lý được minh hoạ tại **Ví dụ 2** (Hình 4) và có danh sách máy chủ như tại **Bảng 3** ở trên:

(i) Xác thực:

STT	Yêu cầu / Máy chủ[26]	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 hoá (nếu không sử dụng)	c) Thiết lập cấu hình máy chủ để bảo đảm 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	+[27]	+	+

[25] Tất cả các thiết bị được nêu trong Bảng 2.
[26] Các máy chủ đã được xác định ở Bảng 3.
[27] 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.

STT	Yêu cầu / Máy chủ[26]	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 hoá (nếu không sử dụng)	c) Thiết lập cấu hình máy chủ để bảo đảm 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.
2	Server 01	+	+	+
3	Server 02	+	+	+
4	[…]	+	+	+

(ii) Kiểm soát truy cập:

STT	Yêu cầu / Máy chủ[28]	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	[…]	+

(iii) Nhật ký hệ thống:

STT	Yêu cầu / Máy chủ[29]	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	[…]	+	+

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

(iv) Phòng, chống xâm nhập:

STT	Yêu cầu / Máy chủ[30]	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[31]	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.

3.2.4. 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 8. Đối với hệ thống thông tin cấp độ 1 có mô hình lô-gic được minh hoạ tại **Ví dụ 1** (Hình 1), mô hình vật lý được minh hoạ tại **Ví dụ 2** (Hình 4) và có danh sách ứng dụng như tại **Bảng 3** ở trên:

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

(i) Xác thực:

STT	Yêu cầu / Ứng dụng[32]	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 hoá thông tin xác thực hệ thống	c) Thiết lập cấu hình ứng dụng để bảo đảm 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 Uỷ ban nhân dân huyện X]	+[33]	+	+
2	[…]	+	+	+

(ii) Kiểm soát truy cập:

STT	Yêu cầu / Ứng dụng[34]	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 Uỷ ban nhân dân huyện X]	+	+
2	[…]	+	+

[32] Các ứng dụng, dịch vụ đã được xác định ở Bảng 3.
[33] 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.
[34] Các ứng dụng, dịch vụ đã được xác định ở Bảng 3.

(iii) Nhật ký hệ thống:

STT	Yêu cầu / Ứng dụng[35]	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 Uỷ 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 thêm các tiêu chí về bảo mật thông tin liên lạc và chống chối bỏ.

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

Lập bảng thuyết minh đáp ứng:

Ví dụ 9. Tiếp tục lấy ví dụ minh hoạ đối với hệ thống thông tin cấp độ 1 có mô hình lô-gic được minh hoạ tại **Ví dụ 1** (Hình 1), mô hình vật lý được minh hoạ tại **Ví dụ 2** (Hình 4) và có danh sách ứng dụng như tại **Bảng 3** 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 hằng ngày (cấu hình sao lưu vào nửa đêm). Định kỳ hằng tuần hoặc hằng tháng tiến hành xoá bớt các file sao lưu, chỉ để lại dữ liệu sao lưu của 7 ngày gần nhất[36].

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.

---

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

TỈNH ỦY LÂM ĐỒNG
VĂN PHÒNG
*

Số 303 - BS/VPTU

V/v Sao Hướng dẫn 26-HD/VPTW, ngày 24/9/2024 của Văn phòng Trung ương Đảng

SAO Y BẢN CHÍNH
Lâm Đồng, ngày 21 tháng 10 năm 2024

Nơi nhận:
- Các huyện, thành ủy, đảng ủy khối trực thuộc,
- Lưu Văn phòng Tỉnh ủy.

PHÓ CHÁNH VĂN PHÒNG

ĐẢNG CỘNG SẢN VIỆT NAM
VĂN PHÒNG
TỈNH ỦY LÂM ĐỒNG

Phạm Ngọc Hà