



HƯỚNG DẪN XÂY DỰNG HỒ SƠ ĐỀ XUẤT CẤP ĐỘ AN TOÀN THÔNG TIN CHO CÁC HỆ THỐNG THÔNG TIN

Đối tượng tập huấn:

- *Sở Thông tin và Truyền thông;*
- *Các đơn vị tham gia triển khai ứng dụng công nghệ thông tin tại các địa phương.*

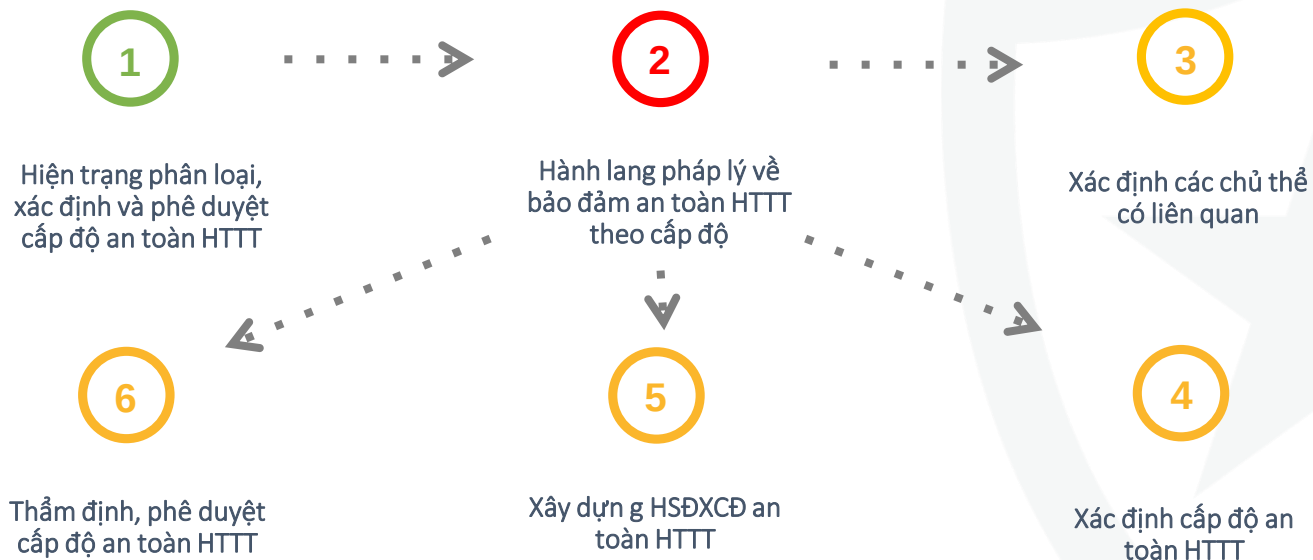
QUAN ĐIỂM CHỈ ĐẠO



- ❖ *An toàn, an ninh mạng là trọng tâm của quá trình chuyển đổi số, là trụ cột quan trọng tạo lập niềm tin số và sự phát triển thịnh vượng trong kỷ nguyên số.*
- ❖ *Chủ quản hệ thống thông tin: Thực hiện nghiêm túc các quy định pháp luật về bảo vệ an ninh mạng; xác định cấp độ và trách nhiệm bảo đảm an toàn hệ thống thông tin theo từng cấp độ và triển khai mô hình bảo vệ 4 lớp trước khi đưa vào sử dụng.*
 - ❑ *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 [964/QĐ-TTg]*



Nội dung trình bày





Nội dung trình bày

1

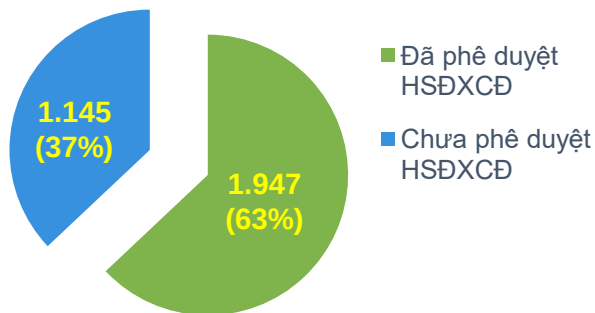
Hiện trạng phân loại,
xác định và phê duyệt
cấp độ an toàn HTTT

Năm 2023

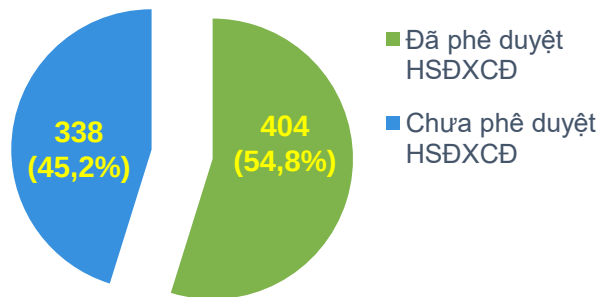
Năm dữ liệu số quốc gia



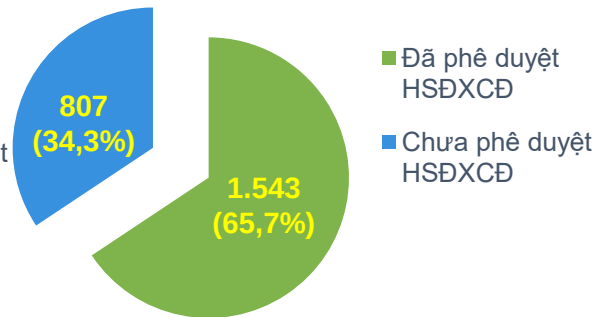
Hiện trạng phân loại, xác định và phê duyệt cấp độ an toàn HTTT (đến hết T4/2023) | Trang 02/55



Toàn quốc: **3.092** HTTT đang vận hành



Bộ, ngành: **742** HTTT đang vận hành



Địa phương: **2.350** HTTT đang vận hành

❑ 15 Bộ, ngành có tỷ lệ phê duyệt HSDXCĐ **thấp, $\leq 50\%$.**

❑ 16 Địa phương có tỷ lệ phê duyệt HSDXCĐ **thấp, $\leq 50\%$.**

- Chủ quản HTTT chưa làm tròn trách nhiệm tại **Điều 20** Nghị định 85/2016/NĐ-CP;
- Đơn vị chuyên trách ATTT chưa làm tròn trách nhiệm tại **Điều 21** Nghị định 85/2016/NĐ-CP;
- Đơn vị vận hành HTTT chưa làm tròn trách nhiệm tại **Điều 22** Nghị định 85/2016/NĐ-CP.

➤ Việc này **có thể bị xử phạt** theo quy định tại Điều 88 của Nghị định số 15/2020/NĐ-CP.



Công tác đơn đốc các Bộ, ngành, địa phương hoàn thành phân loại, phê duyệt cấp độ

Trang 03/55

Thủ tướng Chính phủ yêu cầu

- ✓ Hoàn thành phân loại, xác định và phê duyệt đề xuất cấp độ HTTT **trước 01/12/2022**;
- ✓ Triển khai đầy đủ phương án BDATHTTT theo cấp độ các HTTT đang vận hành **trước 01/6/2023**.

Chỉ thị số 02/CT-TTg
ngày 26/4/2022

Văn bản số 1598/BTTTT-CATTT
ngày 28/4/2022

Bộ TT&TT đề nghị

- ✓ Hoàn thành phê duyệt HSDXCĐ cho tất cả các HTTT **trước ngày 30/6/2022**;
- ✓ Triển khai đầy đủ phương án BDATHTTT theo cấp độ **trước ngày 15/11/2022**;
- ✓ **Cho dừng** các HTTT không BDATTT mạng theo quy định của pháp luật **từ ngày 01/01/2023**.

Bộ TT&TT đề nghị

- ✓ Tập trung rà soát, hoàn thành phân loại, xác định và phê duyệt đề xuất cấp độ ATTT **100% HTTT đang vận hành trước 31/3/2023**;
- ✓ Triển khai đầy đủ phương án bảo đảm ATHTTT theo cấp độ cho **100% HTTT đang vận hành trước ngày 30/9/2023**.

Văn bản số 652/BTTTT-CATTT
ngày 28/02/2023

Mẫu HSDXCĐ tại địa chỉ: <https://ais.gov.vn/thong-tin-tham-khao/mau-hsdxcd.htm>



Nội dung trình bày

1



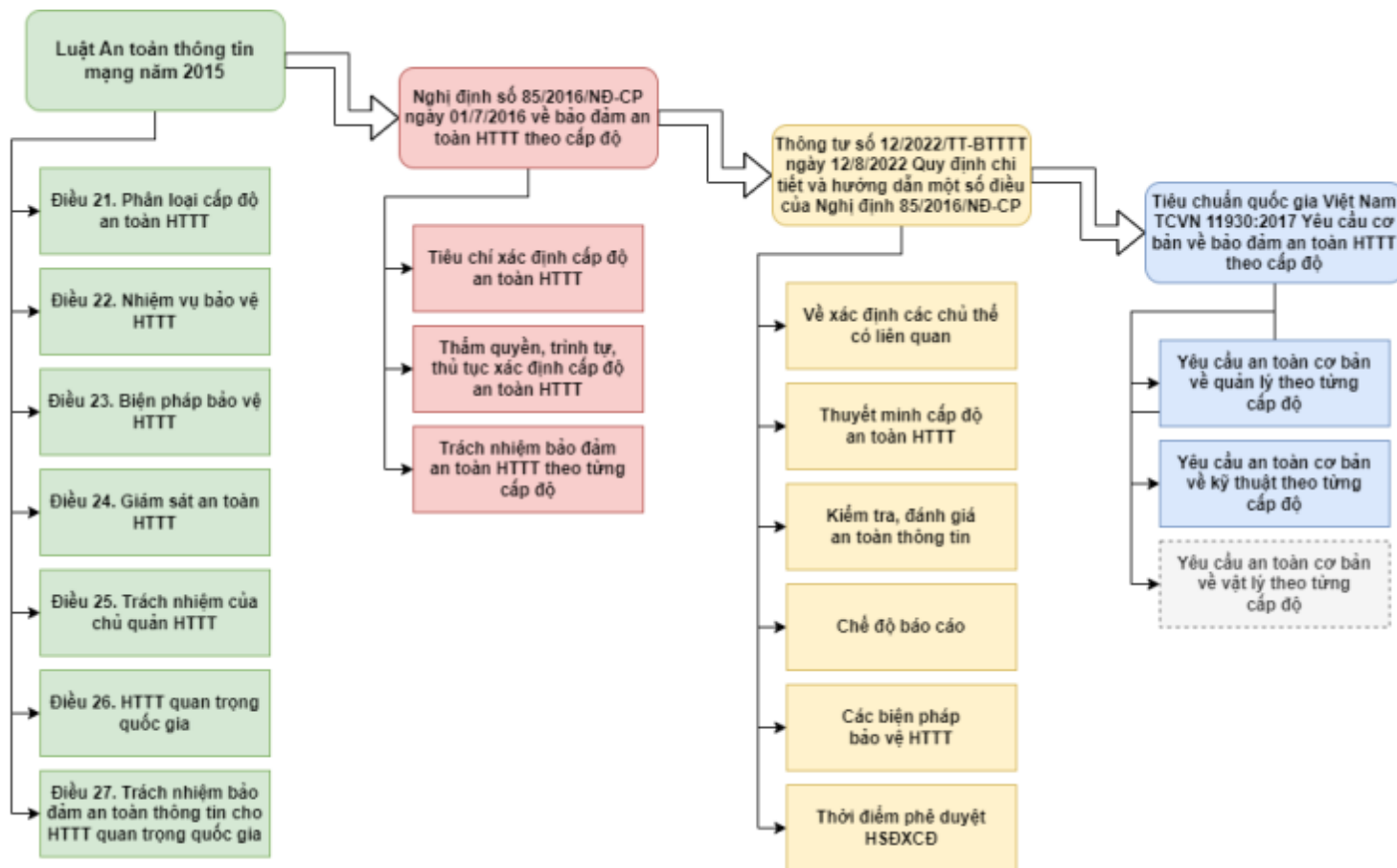
2

Hiện trạng phân loại,
xác định và phê duyệt
cấp độ an toàn HTTT

Hành lang pháp lý về
bảo đảm an toàn HTTT
theo cấp độ

Hành lang pháp lý

Trang 05/55



Bảo đảm an toàn HTTT theo cấp độ là gì?

Trang 06/55



Bảo đảm an toàn hệ thống thông tin theo cấp độ là các hoạt động phân loại cấp độ; xây dựng, thẩm định, phê duyệt hồ sơ đề xuất cấp độ an toàn thông tin cho các hệ thống thông tin và triển khai 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.



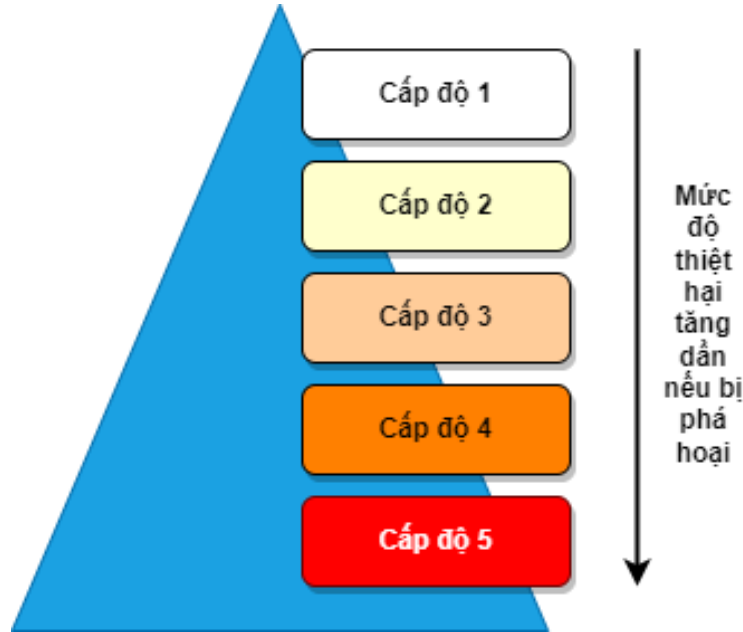
Nguyên tắc cơ bản là việc bảo đảm an toàn hệ thống thông tin theo cấp độ trong hoạt động của cơ quan, tổ chức được thực hiện thường xuyên, liên tục từ khâu thiết kế, xây dựng, vận hành đến khi hủy bỏ; tuân thủ theo tiêu chuẩn, quy chuẩn kỹ thuật.

☐ *Khoản 1 Điều 4 Nghị định 85/2016/NĐ-CP.*



Đây là biện pháp nòng cốt bảo vệ hệ thống thông tin theo quy định tại Luật An toàn thông tin mạng năm 2015.

Phân loại cấp độ an toàn HTTT



- **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;
- **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;
- **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;
- **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;
- **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.

Hệ thống thông tin là gì?



Theo khoản 3 Điều 3 Luật An toàn thông tin mạng năm 2015:

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



Khi đề cập đến hệ thống thông tin là đề cập đến tổng thể *phần mềm* và *hạ tầng triển khai phần mềm*. Nói đến bảo đảm an toàn hệ thống thông tin là nói đến *bảo đảm an toàn thông tin cho phần mềm và hạ tầng triển khai phần mềm*.

Hình thành thông qua hoạt động đầu tư dự án công nghệ thông tin, thuê dịch vụ công nghệ thông tin hoặc các hoạt động triển khai ứng dụng công nghệ thông tin không phải lập dự án.



Các hệ thống sau đây có là hệ thống thông tin?

- Mạng nội bộ của các cơ quan, đơn vị (Mạng LAN);
- Camera giám sát được triển khai nhằm phục vụ hoạt động giám sát an toàn, an ninh trong phạm vi nội bộ tại các cơ quan, đơn vị, trong đó:
 - ☐ Hệ thống camera được thiết lập riêng biệt, độc lập với hạ tầng (mạng nội bộ, đường truyền Internet, thiết bị chuyển mạch, máy chủ) tại cơ quan, đơn vị;
 - ☐ Thông tin thu thập từ camera được lưu trữ, xử lý trên các thiết bị đầu ghi chuyên dụng.

Nguyên tắc thực hiện

- 1 | 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.
- 2 | 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**.
- 3 | 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**.

❏ Điều 4 Nghị định 85/2016/NĐ-CP.



Nội dung trình bày

1

Hiện trạng phân loại,
xác định và phê duyệt
cấp độ an toàn HTTT



2

Hành lang pháp lý về
bảo đảm an toàn HTTT
theo cấp độ



3

Xác định các chủ thể
có liên quan

- 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;
- Chủ đầu tư dự án hoặc hoạt động ứng dụng công nghệ thông tin.



Theo khoản 5 Điều 3 Luật An toàn thông tin mạng, khoản 1 Điều 3 Nghị định số 85/2016/NĐ-CP:

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.

Chủ quản hệ thống thông tin thực thi trách nhiệm tại Điều 20 Nghị định số 85/2016/NĐ-CP.



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.



Điểm c khoản 1 Điều 4 Thông tư số 12/2022/TT-BTTTT:

Ủy ban nhân dân cấp tỉnh *chỉ quyết định chủ quản hệ thống thông tin là cấp có thẩm quyền quyết định đầu tư dự án xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin trong trường hợp đơn vị được giao là chủ quản hệ thống thông tin đã được đánh giá có đủ năng lực để thực thi đầy đủ các quy định tại Điều 20 Nghị định 85/2016/NĐ-CP.*



Theo khoản 5 Điều 3 Nghị định số 85/2016/NĐ-CP:

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 (*Chủ quản hệ thống thông tin chỉ định đơn vị trực thuộc phù hợp*). Đơn vị chuyên trách về an toàn thông tin thực thi trách nhiệm tại Điều 21 Nghị định số 85/2016/NĐ-CP.



Đối với các cơ quan, tổ chức được xác định là chủ quản hệ thống thông tin nhưng chưa có đơn vị chuyên trách về an toàn thông tin độc lập, thì đơn vị chuyên trách về an toàn thông tin là *Đơn vị chuyên trách về công nghệ thông tin*.

- ☐ Đối với Ủy ban nhân dân cấp tỉnh: Sở Thông tin và Truyền thông;
- ☐ Đối với Ủy ban nhân dân cấp huyện: Phòng Văn hóa – Thông tin.

Xác định Đơn vị vận hành HTTT



Theo khoản 3 Điều 3 Nghị định số 85/2016/NĐ-CP:

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.

Đơn vị vận hành hệ thống thông tin thực thi trách nhiệm tại Điều 22 Nghị định số 85/2016/NĐ-CP.



Trong trường hợp Chủ quản hệ thống thông tin thuê ngoài dịch vụ công nghệ thông tin, Đơn vị vận hành hệ thống thông tin là *bên cung cấp dịch vụ*.



Khoản 3 Điều 4 Thông tư số 12/2022/TT-BTTTT: Trường hợp cần thiết, chủ quản hệ thống thông tin có thể ủy quyền cho một tổ chức trực thuộc có đủ năng lực để thay mặt thực hiện trách nhiệm của chủ quản hệ thống thông tin quy định tại khoản 2 Điều 20 Nghị định 85/2016/NĐ-CP. Việc ủy quyền phải được thực hiện bằng văn bản, trong đó nêu rõ phạm vi của hệ thống, trách nhiệm của tổ chức được ủy quyền và thời hạn ủy quyền.



Chỉ nêu vấn đề ủy quyền thực hiện trách nhiệm của chủ quản HTTT quy định tại khoản 2 Điều 20 mà ủy quyền thực hiện quy định tại khoản 1 Điều 20 Nghị định 85/2016/NĐ-CP, do đó:

- ☐ Đơn vị được ủy quyền chỉ thực hiện các nhiệm vụ được ủy quyền mà không phải Đơn vị được ủy quyền trở thành chủ quản của HTTT;
- ☐ Đơn vị chuyên trách về an toàn thông tin vẫn thực hiện trách nhiệm của mình đối với HTTT.



Chỉ ủy quyền trách nhiệm chủ quản hệ thống thông tin trong trường hợp HTTT được đề xuất cấp độ 1, 2 hoặc 3 và đơn vị trực thuộc được ủy quyền có đủ năng lực để thay mặt thực hiện trách nhiệm được quy định tại khoản 2 Điều 20 Nghị định 85/2016/NĐ-CP.

Giao đơn vị chuyên trách về an toàn thông tin đánh giá năng lực của từng đơn vị dự kiến được giao là chủ quản hệ thống thông tin hoặc dự kiến được ủy quyền thực hiện trách nhiệm của chủ quản hệ thống thông tin.

Phân cấp đầu tư ứng dụng CNTT



Khi dự kiến xác định sở, ban, ngành cụ thể, được phân cấp đầu tư ứng dụng công nghệ thông tin là Chủ quản hệ thống thông tin thì sở, ban, ngành đó cần chỉ định 01 đơn vị trực thuộc là Đơn vị chuyên trách về an toàn thông tin để triển khai các nhiệm vụ thuộc trách nhiệm của đơn vị chuyên trách về an toàn thông tin theo quy định tại Nghị định số 85/2016/NĐ-CP.



Đơn vị chuyên trách về an toàn thông tin thực thi các nhiệm vụ được quy định tại Điều 21 Nghị định số 85/2016/NĐ-CP, trong đó có: Thẩm định HSĐXCĐ 1, 2, 3, cho ý kiến chuyên môn về an toàn thông tin đối với HSĐXCĐ 4, 5; ban hành quyết định phê duyệt cấp độ an toàn thông tin đối với hệ thống thông tin tin được đề xuất cấp độ 1, 2. Do đó, **Chủ quản hệ thống thông tin phải chỉ định đơn vị có tư cách pháp nhân làm Đơn vị chuyên trách về an toàn thông tin.**



Trường hợp theo cơ cấu tổ chức, sở, ban, ngành là cấp có thẩm quyền thẩm quyền quyết định đầu tư xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin *không có đơn vị trực thuộc* có tư cách pháp nhân, hoặc có nhưng không đủ năng lực thực thi các quy định tại Điều 21 Nghị định số 85/2016/NĐ-CP thì sở, ban, ngành cần báo cáo Ủy ban nhân dân tỉnh để Ủy ban nhân dân tỉnh đóng vai trò làm Chủ quản hệ thống thông tin và Sở Thông tin và Truyền thông là Đơn vị chuyên trách về an toàn thông tin.

1

Trong giai đoạn chuẩn bị đầu tư, xây dựng dự án, hoạt động ứng dụng công nghệ thông tin:

Chủ đầu tư dự án, hoạt động ứng dụng công nghệ thông tin phục vụ xây dựng mới hệ thống thông tin đóng vai trò là đơn vị vận hành hệ thống thông tin.

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:

- ☐ 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;
- ☐ Đơn vị vận hành hệ thống thông tin nếu được Chủ quản hệ thống thông tin giao nhiệm vụ;
- ☐ Đơn vị tham gia sử dụng hệ thống thông tin nếu không được chủ quản hệ thống thông tin giao nhiệm vụ là đơn vị vận hành hệ thống thông tin. Khi đó quy chế bảo đảm an toàn hệ thống 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.



Nội dung trình bày

1

Hiện trạng phân loại,
xác định và phê duyệt
cấp độ an toàn HTTT



2

Hành lang pháp lý về
bảo đảm an toàn HTTT
theo cấp độ



3

Xác định các chủ thể
có liên quan



4

Xác định cấp độ an
toàn HTTT

Nguyên tắc xác định cấp độ

1

- Hệ thống thông tin **chỉ có một** Chủ quản hệ thống thông tin;
- 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.

□ Điều 5 Nghị định 85/2016/NĐ-CP.



Bước 1: Xác định hệ thống thông tin



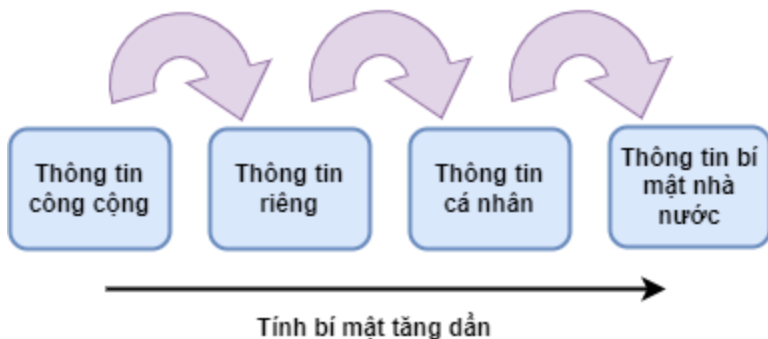
Trước hết cần làm rõ các thông tin sau đây:

- **Tên hệ thống thông tin:** Dựa trên nội dung thuyết minh trong chủ trương đầu tư hoặc 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 CNTT, đảm bảo thuyết minh thống nhất;
- **Các thành phần cấu thành hệ thống thông tin,** đảm bảo ứng dụng công nghệ thông tin đáp ứng các tiêu chí hình thành hệ thống thông tin;
- **Các chủ thể có liên quan** gồm: Chủ quản hệ thống thông tin, đơn vị chuyên trách an toàn thông tin của chủ quản hệ thống thông tin, đơn vị vận hành.



- ❑ Các trường hợp ứng dụng CNTT **không đáp ứng tiêu chí** là hệ thống thông tin, **không phải xác định cấp độ an toàn hệ thống thông tin.**
- ❑ Trường hợp hệ thống thông tin được hình thành bởi **nhiều hệ thống thông tin thành phần:** Cần thực hiện các bước xác định cấp độ an toàn thông tin đối với từng hệ thống thông tin thành phần, sau đó, cấp độ an toàn thông tin đối với hệ thống thông tin chính được xác định là cấp độ cao nhất trong các cấp độ của các hệ thống thành phần cấu thành.

Bước 2: Phân loại thông tin



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

❑ Khi xác định cấp độ an toàn hệ thống 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: Hệ thống 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.

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:

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;
- b) Hệ thống thư điện tử;
- c) Hệ thống quản lý văn bản và điều hành;
- d) Hệ thống họp, hội nghị trực tuyến;
- đ) Hệ thống đào tạo trực tuyến;
- 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 như hệ thống thông tin phục vụ người dân, doanh nghiệp.

Bước 3: Phân loại hệ thống thông tin (2)

| Trang 22/55

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

- a) Trang, cổng thông tin điện tử phục vụ người dân, doanh nghiệp;
- b) Hệ thống thư điện tử dùng chung cho người dân, doanh nghiệp;
- c) Hệ thống quản lý văn bản và điều hành dùng chung cho người dân, doanh nghiệp;
- d) Hệ thống họp, hội nghị trực tuyến dùng chung cho người dân, 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 hoặc hỗ trợ cung cấp dịch vụ trực tuyến;
- h) Hệ thống chăm sóc khách hàng, tiếp nhận phản ánh kiến nghị, khảo sát, thu thập thông tin, đánh giá mức độ phục vụ người dân và doanh nghiệp;
- i) Hệ thống cung cấp dữ liệu mở;
- k) Hệ thống phục vụ cơ chế một cửa quốc gia.

Lưu ý:

- Trong khái niệm về hệ thống thông tin phục vụ người dân, doanh nghiệp được nêu ở trên, **dịch vụ trực tuyến** 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.
- 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. Ví dụ: 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).

Bước 3: Phân loại hệ thống thông tin (3)

Hệ thống cơ sở hạ tầng thông tin là tập hợp trang thiết bị, đường truyền dẫn kết nối phục vụ chung hoạt động của nhiều cơ quan, tổ chức (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) Hệ thống hợp, hội nghị trực tuyến dùng chung của nhiều cơ quan, tổ chức;
- c) Trung tâm dữ liệu, điện toán đám mây;
- d) Hệ thống giám sát điều hành thông minh (IOC);
- đ) Hệ thống giám sát điều hành an toàn thông tin mạng (SOC);
- e) Hệ thống định danh, xác thực điện tử, chứng thực điện tử, chữ ký số;
- g) Hệ thống kết nối tích hợp, chia sẻ dữ liệu giữa các hệ thống thông tin;
- h) Hệ thống giám sát, điều hành hoạt động của hệ thống thông tin điều khiển công nghiệp;
- i) Hệ thống tổng hợp, phân tích dữ liệu;
- k) Cơ sở dữ liệu tập trung;
- l) Hệ thống lưu trữ, sao lưu dữ liệu tập trung;
- m) 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 thuộc 11 lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng theo Quyết định số 632/QĐ-TTg ngày 10/5/2017 của Thủ tướng Chính phủ.

Bước 3: Phân loại hệ thống thông tin (4)

| Trang 24/55

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.

Hệ thống thông tin khác là các hệ thống thông tin không thuộc các hệ thống thông tin được mô tả tại các mục 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.

Khoản 7 Điều 7 Thông tư số 12/2022/2022:

Định kỳ hàng quý (ngày đầu tiên của quý), Cục An toàn thông tin - Bộ Thông tin và Truyền thông có trách nhiệm cập nhật, bổ sung danh mục các hệ thống thông tin theo phân loại các hệ thống thông tin và công bố trên Cổng thông tin điện tử của Bộ Thông tin và Truyền thông.

Bước 4: Xác định cấp độ

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**, trong đó, **cần lưu ý xác định rõ quy mô và phạm vi triển khai của HTTT**, cụ thể:

1) Hệ thống thông tin cấp độ 1: Căn cứ Điều 7 Nghị định số 85/2016/NĐ-CP, hệ thống thông tin cấp độ 1 là:

- **Tiêu chí:** 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:** 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.

2) Hệ thống thông tin cấp độ 2: Căn cứ Điều 8 Nghị định số 85/2016/NĐ-CP, hệ thống thông tin cấp độ 2 là hệ thống thông tin có 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: Trang, cổng thông tin điện tử của cơ quan, tổ chức có xử lý thông tin riêng, thông tin cá nhân người sử dụng; Hệ thống quản lý văn bản và điều hành, phần mềm quản lý cán bộ, hệ thống thư điện tử, hệ thống họp, hội nghị trực tuyến... phục vụ hoạt động nội bộ của một cơ quan, đơn vị hoặc được triển khai trên phạm vi một bộ, một tỉnh; Hệ thống quản lý khám chữa bệnh chưa tích hợp các giải pháp cung cấp hoặc hỗ trợ cung cấp dịch vụ đăng ký khám chữa bệnh trực tuyến tại các bệnh viện...

Bước 4: Xác định cấp độ (2)

2) Hệ thống thông tin cấp độ 2 (tiếp):

(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 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: Trang, cổng thông tin điện tử của cơ quan, tổ chức có cung cấp các dịch vụ trực tuyến cho người dân, doanh nghiệp; 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 số người sử dụng; Hệ thống quản lý khám chữa bệnh đã tích hợp các giải pháp cung cấp hoặc hỗ trợ cung cấp các dịch vụ đăng ký khám chữa bệnh trực tuyến tại các bệnh viện trong đó số bệnh nhân đã đăng ký khám chữa bệnh trực tuyến là dưới 10.000 người...

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

Ví dụ: Trung tâm dữ liệu, Hệ thống tổng hợp, phân tích dữ liệu nội bộ của một cơ quan, tổ chức...

Bước 4: Xác định cấp độ (3)

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.

(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 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: Cổng dịch vụ công, hệ thống một cửa điện tử cấp bộ, cấp tỉnh; 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 đã được triển khai phạm vi rộng với hơn 10.000 người sử dụng; Hệ thống thương mại điện tử; Hệ thống quản lý khám chữa bệnh đã tích hợp các giải pháp cung cấp hoặc hỗ trợ cung cấp các dịch vụ đăng ký khám chữa bệnh trực tuyến tại các bệnh viện trong đó số bệnh nhân đã đăng ký khám chữa bệnh trực tuyến từ 10.000 người trở lên...

(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 hoặc một số tỉnh.

Ví dụ: Trung tâm dữ liệu cấp bộ, cấp tỉnh; Nền tảng tích hợp, chia sẻ dữ liệu cấp Bộ, cấp tỉnh; Mạng truyền số liệu chuyên dùng cấp II tại các địa phương...

(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.



Nội dung trình bày

1

Hiện trạng phân loại,
xác định và phê duyệt
cấp độ an toàn HTTT



2

Hành lang pháp lý về
bảo đảm an toàn HTTT
theo cấp độ



5

Xây dựng HSĐXCĐ an
toàn HTTT



3

Xác định các chủ thể
có liên quan



4

Xác định cấp độ an
toàn HTTT

1

Hồ sơ đề xuất cấp độ an toàn hệ thống thông tin **được xem là nền tảng** để triển khai tất cả các biện pháp bảo đảm an toàn thông tin cho hệ thống thông tin theo quy định của pháp luật; là căn cứ để xác định các hạng mục, giải pháp khi đầu tư, thuê hoặc mua dịch vụ an toàn thông tin cho hệ thống thông tin, đồng thời, là tài liệu để đánh giá mức độ tuân thủ pháp luật về an toàn thông tin mạng đối với hệ thống thông tin theo quy định.

2

Căn cứ các quy định tại Điều 15 Nghị định số 85/2016/NĐ-CP và khoản 2 Điều 8 Thông tư số 12/2022/TT-BTTTT, Tài liệu thuyết minh hồ sơ đề xuất cấp độ gồm các tài liệu thành phần sau:

- Tài liệu mô tả, thuyết minh tổng quan về hệ thống thông tin;
- Tài liệu thuyết minh về việc đề xuất cấp độ;
- Tài liệu thuyết minh phương án bảo đảm an toàn thông tin theo cấp độ tương ứng.

Mẫu HSDXCĐ tại địa chỉ: <https://ais.gov.vn/thong-tin-tham-khao/mau-hsdxcd.htm>

Khi nào cần xây dựng HSĐXCĐ?

Căn cứ quy định tại Điều 13, Điều 14 và Điều 18 Nghị định số 85/2016/NĐ-CP, các trường hợp sau đây cần xây dựng HSĐXCĐ:

- a) Ngay sau khi được cấp có thẩm quyền **phê duyệt chủ trương** xây dựng mới HTTT và chủ đầu tư **tiến hành xây dựng** Báo cáo kinh tế - kỹ thuật (trong trường hợp dự án đầu tư áp dụng phương án thiết kế 01 bước) hoặc 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);
- b) HTTT **đang vận hành nhưng chưa được phê duyệt cấp độ** an toàn thông tin;
- c) HTTT **đang vận hành đã được phê duyệt cấp độ** nhưng được cập nhật, mở rộng hoặc qua rà soát thấy cần phải cập nhật, điều chỉnh HSĐXCĐ (điều chỉnh cấp độ hoặc các phương án bảo đảm ATTT) thì cần điều chỉnh, cập nhật nội dung HSĐXCĐ.

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

Lưu ý: Để việc xây dựng HSĐXCĐ cho HTTT 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 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 cho phù hợp.

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

Căn cứ quy định tại khoản 1, khoản 2 Điều 13 Nghị định số 85/2016/NĐ-CP và khoản 1 Điều 8 Thông tư số 12/2022/TT-BTTTT:

Ngay sau khi được cấp có thẩm quyền **phê duyệt chủ trương** xây dựng mới hoặc nâng cấp mở rộng HTTT và **Chủ đầu tư tiến hành xây dựng** Tài liệu thiết kế hệ thống thông tin, bao gồm 01 trong các tài liệu:

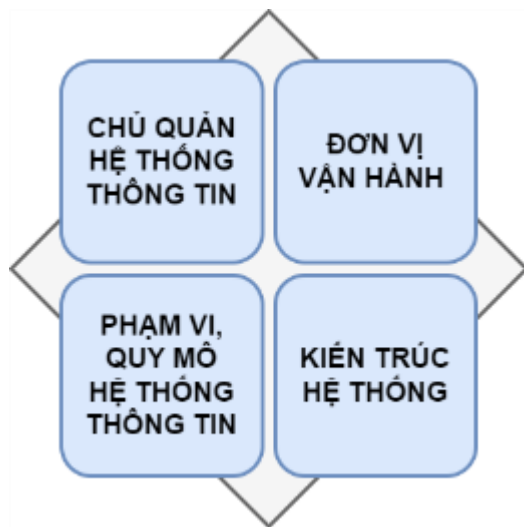
- Báo cáo kinh tế - kỹ thuật (trong trường hợp dự án đầu tư áp dụng phương án thiết kế 01 bước) hoặc;
- Báo cáo nghiên cứu khả thi (trong trường hợp dự án đầu tư áp dụng phương án thiết kế 02 bước) hoặc;
- Kế hoạch thuê dịch vụ công nghệ thông tin (trong trường hợp áp dụng hình thức thuê dịch vụ công 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),

Chủ đầu tư cần thực hiện:

- ☐ Xây dựng mới hoặc điều chỉnh, cập nhật nội dung HSĐXCĐ cho hệ thống thông tin;
- ☐ **Lồng ghép các nội dung thuyết minh đề xuất cấp độ được thuyết minh trong HSĐXCĐ vào Tài liệu thiết kế HTTT đảm bảo phương án kỹ thuật trong Tài liệu thiết kế HTTT phải đáp ứng các yêu cầu của phương án bảo đảm an toàn thông tin theo cấp độ được đề xuất, được thuyết minh trong HSĐXCĐ.**

Cần xây dựng mới hoặc điều chỉnh, cập nhật nội dung HSĐXCĐ song song với việc xây dựng tài liệu thiết kế khi thực hiện xây dựng mới hoặc nâng cấp mở rộng HTTT.

Thuyết minh tổng quan về HTTT



Căn cứ quy định tại khoản 3 Điều 8 Thông tư số 12/2022/TT-BTTTT:

1) 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).

2) 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).

3) 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.

4) 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)).

Thuyết minh về việc đề xuất cấp độ



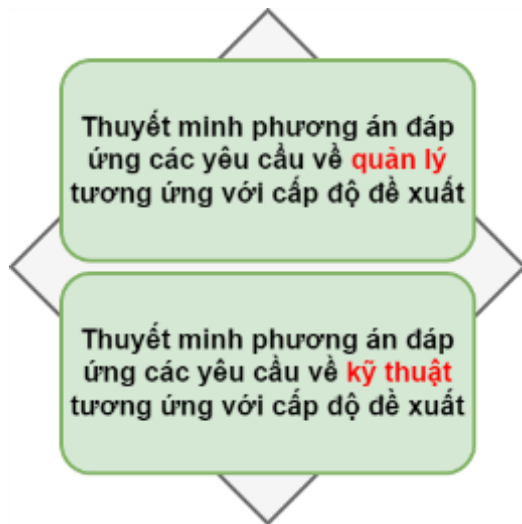
Căn cứ quy định tại khoản 4 Điều 8 Thông tư số 12/2022/TT-BTTTT:

1) 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.

STT	Tên hệ thống thông tin	Cấp độ đề xuất	Căn cứ đề xuất cấp độ
1	...	...	...
2	...	...	...
3	...	...	...

2) Thuyết minh chi tiết đối với các HTTT, 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 HTTT.

3) Đối với hệ thống thông tin được đề xuất cấp độ 4 hoặc cấp độ 5, cần làm rõ thêm một số nội dung, chi tiết xem tại khoản 5 Điều 8 Thông tư số 12/2022/TT-BTTTT.



Căn cứ quy định tại khoản 6 Điều 8, Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT:

1) Yêu cầu cơ bản về quản lý, bao gồm:

- a) Thiết lập chính sách an toàn thông tin;
- b) Tổ chức bảo đảm an toàn thông tin;
- c) Bảo đảm nguồn nhân lực;
- d) Quản lý thiết kế, xây dựng hệ thống;
- đ) Quản lý vận hành hệ thống;
- e) *Phương án Quản lý rủi ro an toàn thông tin;*
- g) *Phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin.*

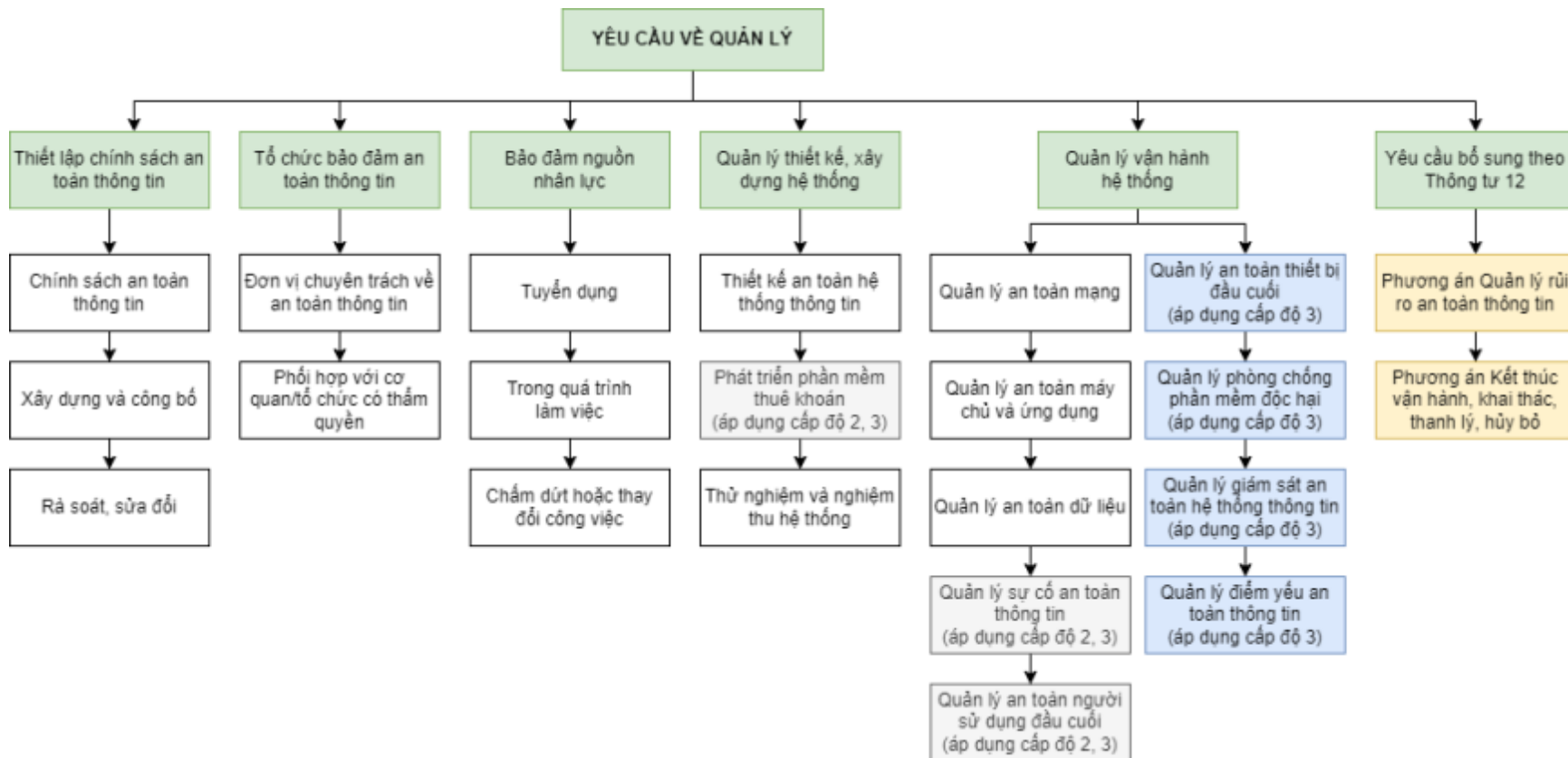
2) Yêu cầu cơ bản về kỹ thuật, bao gồm:

- a) Bảo đảm an toàn mạng;
- b) Bảo đảm an toàn máy chủ;
- c) Bảo đảm an toàn ứng dụng;
- d) Bảo đảm an toàn dữ liệu.

Chi tiết yêu cầu đối với từng cấp độ được quy định tại các Phụ lục I, II, III, IV, V Thông tư 12/2022/TT-BTTTT.

Thuyết minh đáp ứng các yêu cầu quản lý

Trang 35/55



Theo quy định tại khoản 7 Điều 9 Thông tư số 12/2022/TT-BTTTT:

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

Lưu ý:

- ❑ *Mỗi hệ thống thông tin cần có một quy chế bảo đảm an toàn thông tin đáp ứng các yêu cầu an toàn về quản lý theo cấp độ an toàn hệ thống thông tin tương ứng:* Việc này là hoàn toàn phù hợp, giúp đưa ra các chính sách về quản lý *đảm bảo thực thi các phương án bảo đảm an toàn hệ thống 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 TCVN 11930:2017;
- ❑ *Quy chế bảo đảm an toàn thông tin cho hệ thống thông tin phải được cấp có thẩm quyền phê duyệt, ban hành trước khi Hồ sơ đề xuất cấp độ được phê duyệt:* Việc này cũng là hợp lý, *vì mỗi tiêu chí bảo đảm an toàn thông tin về quản lý theo cấp độ tương ứng cần được thực thi bởi một biện pháp cụ thể*. Do đó, để biện pháp có thể được thực thi trong thực tiễn, cấp có thẩm quyền cần ban hành văn bản là căn cứ để thực hiện. Do đó, 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 bảo đảm an toàn thông tin 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*.

Quy chế bảo đảm an toàn hệ thống thông tin theo Thông tư số 12/2022/TT-BTTTT, có cần ban hành hay không khi đã có quy chế quản lý, sử dụng, vận hành hệ thống thông tin (đã có nội dung đảm bảo an toàn thông tin)?

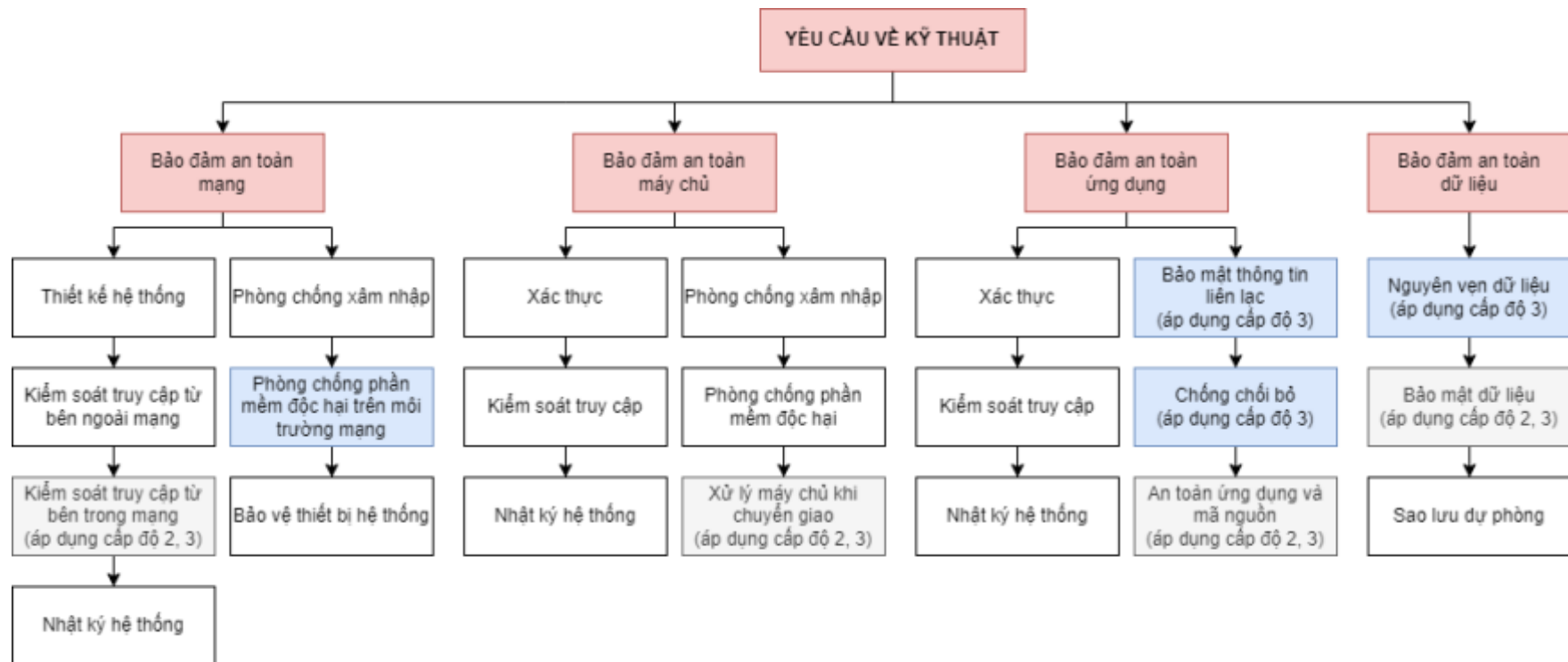
Trả lời:

Thông tư số 12/2022/TT-BTTTT **không bắt buộc** mỗi HTTT phải ban hành riêng 01 quy chế bảo đảm an toàn thông tin, do đó:

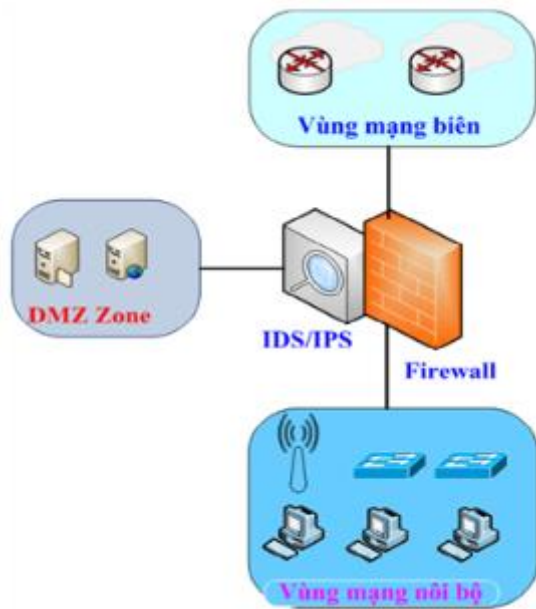
- ☐ Trường hợp Chủ quản hệ thống thông tin hoặc Đơn vị vận hành **đã ban hành quy chế** quản lý, sử dụng, vận hành HTTT, trong đó đã có đầy đủ các nội dung đảm bảo an toàn thông tin **phù hợp với tất cả các tiêu chí** bảo đảm an toàn thông tin về quản lý theo tất cả các cấp độ 1 (18 tiêu chí), cấp độ 2 (42 tiêu chí), cấp độ 3 (80 tiêu chí) tương ứng (hoặc cấp độ 4 (96 tiêu chí), cấp độ 5 (103 tiêu chí) nếu có hệ thống thông tin tương ứng đề xuất cấp độ 4, 5), **đảm bảo thực thi trong thực tiễn** thì có thể áp dụng đối với tất cả các hệ thống thông tin mà không cần xây dựng quy chế bảo đảm an toàn thông tin mới.
- ☐ Trường hợp quy chế chung không đáp ứng yêu cầu thì cần xây dựng bổ sung các chính sách theo phương án ban hành quy chế chung sửa đổi bổ sung hoặc quy chế mới thay thế quy chế hiện tại hoặc có thể ban hành các quy chế riêng cho nhóm các hệ thống thông tin có liên quan.

Thuyết minh đáp ứng các yêu cầu kĩ thuật

Trang 38/55



Yêu cầu thiết kế HTTT: HTTT cấp độ 1



Thiết kế 03 phương án bảo đảm an toàn thông tin / 03 vùng mạng:

Phương án thiết kế bảo đảm các yêu cầu sau:

- 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;
- 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;
- 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.

- ☐ **Vùng mạng nội bộ (LAN):** Vùng mạng này 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;
- ☐ **Vùng mạng biên (outside zone):** Vùng mạng được thiết lập để cung cấp các kết nối hệ thống ra bên ngoài Internet và các mạng khác;
- ☐ **Vùng DMZ (demilitarized zone):** 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.

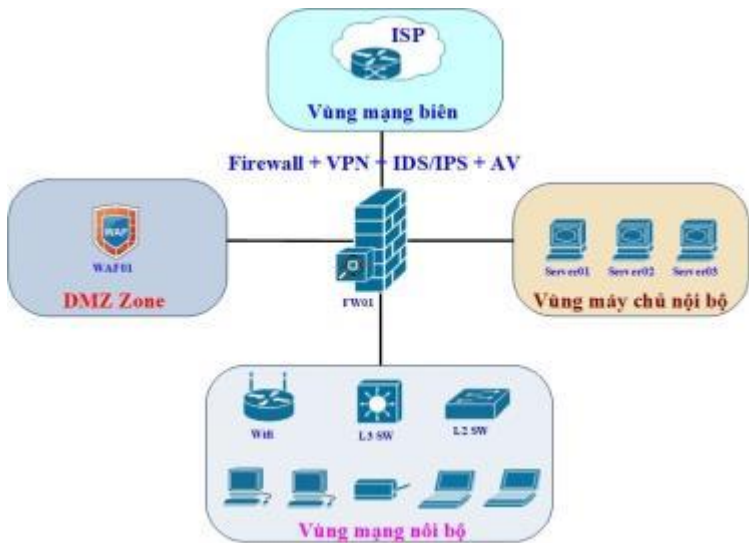
Yêu cầu thiết kế HTTT: HTTT cấp độ 2

Trang 40/55

Thiết kế 06 phương án bảo đảm an toàn thông tin / 06 vùng mạng:

Phương án thiết kế bảo đảm các yêu cầu sau:

- 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;
- 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;
- 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;
- Có phương án phòng chống tấn công mạng cho ứng dụng web; sử dụng sản phẩm Tường lửa ứng dụng web đối với HTTT theo quy định tại khoản 2 Điều 8 Nghị định 85/2016/NĐ-CP;
- Có phương án BĐATTT cho hệ thống thư điện tử đối với hệ thống thư điện tử;
- Có phương án dự phòng cho các thiết bị mạng chính, bao gồm thiết bị chuyển mạch trung tâm hoặc tương đương, thiết bị tường lửa trung tâm.



- ☐ **Vùng máy chủ nội bộ (internal server zone):** 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;
- ☐ **Vùng mạng không dây (nếu có)** tách riêng, độc lập với các vùng mạng khác.

Yêu cầu thiết kế HTTT: HTTT cấp độ 3

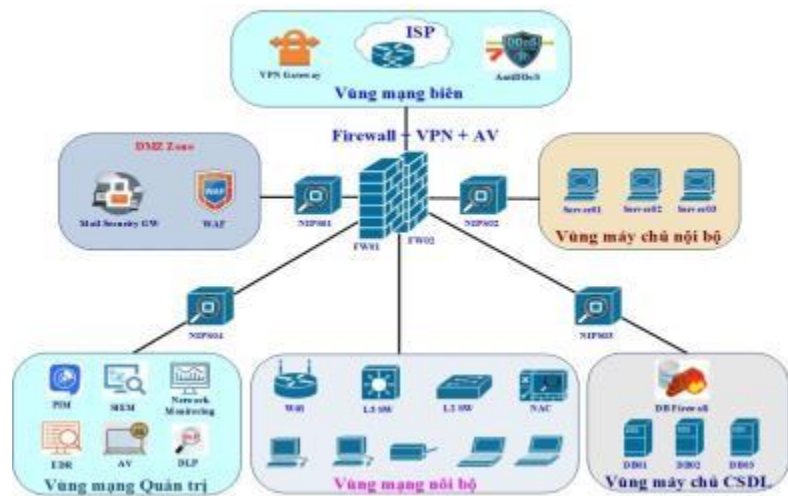
Trang 41/55

Thiết kế 16 phương án bảo đảm an toàn thông tin / 07 vùng mạng:

Phương án thiết kế bảo đảm các yêu cầu sau:

- Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn sử dụng mạng riêng ảo hoặc phương án tương đương; sử dụng sản phẩm Mạng riêng ảo đối với hệ thống thông tin có xử lý thông tin bí mật nhà nước hoặc hệ thống thông tin quy định tại điểm c khoản 2 Điều 9 Nghị định 85/2016/NĐ-CP;
- Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập sử dụng sản phẩm Tường lửa có tích hợp chức năng phòng, chống xâm nhập hoặc sản phẩm Phòng, chống xâm nhập lớp mạng;
- Có phương án cân bằng tải, dự phòng nóng cho các thiết bị mạng chính, tối thiểu gồm thiết bị chuyển mạch trung tâm hoặc tương đương, thiết bị tường lửa trung tâm, tường lửa ứng dụng web, hệ thống lưu trữ tập trung, tường lửa cơ sở dữ liệu (nếu có);
- Có phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu; sử dụng sản phẩm Tường lửa cơ sở dữ liệu đối với hệ thống cơ sở dữ liệu tập trung, đáp ứng tiêu chí quy định tại khoản 3 Điều 9 Nghị định 85/2016/NĐ-CP;

- Vùng mạng máy chủ cơ sở dữ liệu (database server zone):** 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;
- Vùng quản trị (management zone):** 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.



Yêu cầu thiết kế HTTT: HTTT cấp độ 3 (2)

Trang 42/55

Thiết kế 16 phương án bảo đảm an toàn thông tin / 07 vùng mạng:

Phương án thiết kế bảo đảm các yêu cầu sau (tiếp):

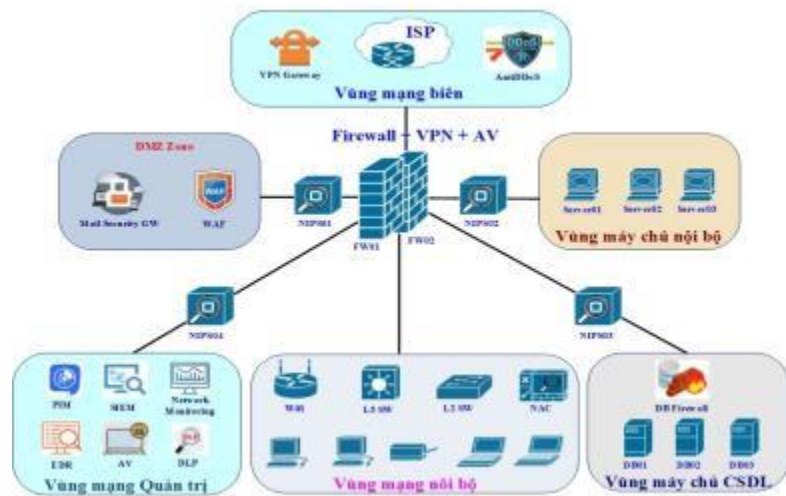
v. Có phương án chặn lọc phần mềm độc hại trên môi trường mạng sử dụng Tường lửa tích hợp chức năng phòng, chống mã độc trên môi trường mạng hoặc phương án tương đương;

vi. Có phương án phòng chống tấn công từ chối dịch vụ; sử dụng dịch vụ của doanh nghiệp hoặc sản phẩm Phòng, chống tấn công từ chối dịch vụ đối với các hệ thống Trung tâm dữ liệu, điện toán đám mây, hệ thống Định danh, xác thực điện tử, chứng thực điện tử, chữ ký số và hệ thống Kết nối tích hợp, chia sẻ dữ liệu, đáp ứng tiêu chí quy định tại khoản 3 Điều 9 Nghị định 85/2016/NĐ-CP;

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

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

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



Yêu cầu thiết kế HTTT: HTTT cấp độ 3 (3)

Trang 43/55

Thiết kế 16 phương án bảo đảm an toàn thông tin / 07 vùng mạng:

Phương án thiết kế bảo đảm các yêu cầu sau (tiếp):

- x. Có phương án giám sát hệ thống thông tin tập trung;
- xi. Có phương án giám sát an toàn hệ thống thông tin tập trung sử dụng sản phẩm Quản lý và phân tích sự kiện an toàn thông tin hoặc sản phẩm tương đương;
- xii. Có phương án quản lý sao lưu dự phòng tập trung sử dụng hệ thống lưu trữ tập trung và sản phẩm quản lý lưu trữ tập trung;
- xiii. Có phương án quản lý phần mềm phòng chống mã độc trên máy chủ/máy tính người dùng, sử dụng sản phẩm Phòng, chống mã độc và/hoặc sản phẩm Phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu cuối, có chức năng quản lý tập trung;
- xiv. Có phương án phòng, chống thất thoát dữ liệu; sử dụng sản phẩm Phòng, chống thất thoát dữ liệu đối với hệ thống thông tin có xử lý thông tin bí mật nhà nước hoặc hệ thống thông tin quy định tại điểm c khoản 2 Điều 9 Nghị định 85/2016/NĐ-CP;
- xv. Có phương án dự phòng kết nối mạng Internet cho các máy chủ dịch vụ;
- xvi. Có phương án bảo đảm an toàn cho mạng không dây (nếu có).



Yêu cầu thiết kế HTTT: HTTT cấp độ 3 (4)

Trang 44/55

Đối với hệ thống thông tin được đề xuất cấp độ 3 tại sao Tiêu chuẩn quốc gia TCVN 11930:2017 chỉ yêu cầu 13 phương án kỹ thuật còn tại Phụ lục III Thông tư số 12/2022/TT-BTTTT nêu 16 phương án kỹ thuật?

Trả lời:

So với Tiêu chuẩn quốc gia TCVN 11930:2017, tại Phụ lục III Thông tư số 12/2022/TT-BTTTT có bổ sung 03 phương án BĐATTT cho cấp độ 3 gồm:

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

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

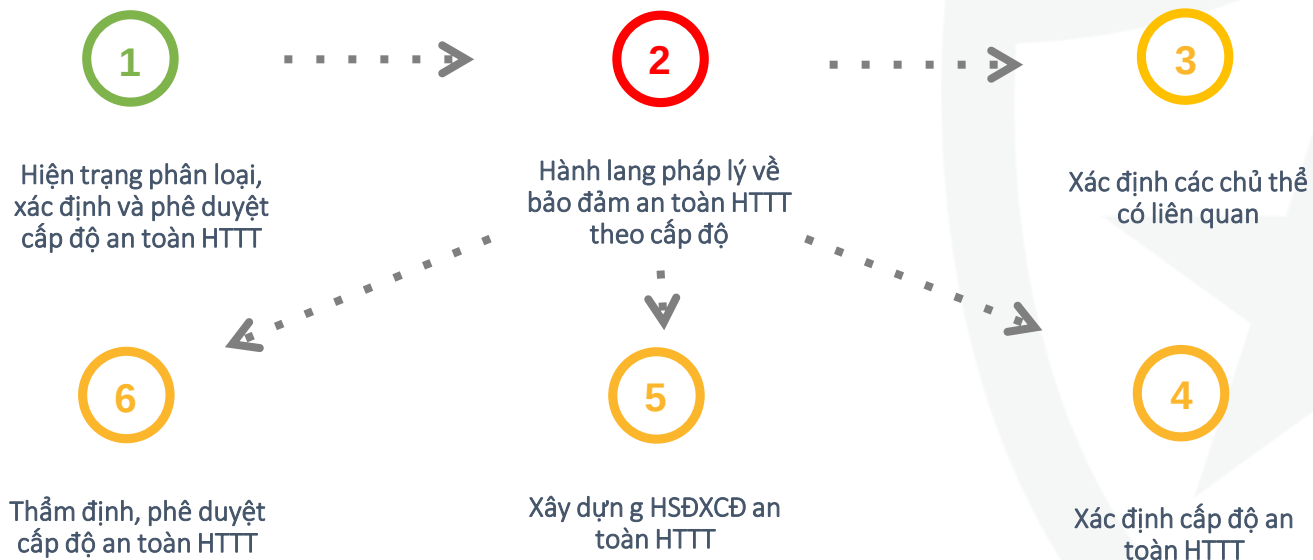
ix. Có phương án quản lý truy cập lớp mạng; sử dụng sản phẩm Quản lý truy cập lớp mạng đối với hệ thống Mạng nội bộ, Trung tâm giám sát điều hành an toàn thông tin mạng, đáp ứng tiêu chí quy định tại khoản 3 Điều 9 Nghị định 85/2016/NĐ-CP.

Việc bổ sung này để phù hợp với yêu cầu thực tế. Tuy nhiên, các biện pháp được bổ sung cũng chỉ yêu cầu với một số loại hình hệ thống thông tin cụ thể, được chỉ rõ trong Thông tư, không phải 100% hệ thống thông tin cấp độ 3 đều phải thực hiện đầy đủ 16 phương án bảo đảm an toàn thông tin.





Nội dung trình bày



Thẩm quyền thẩm định, phê duyệt cấp độ

| Trang 46/55

1,2

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

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 hồ sơ đề xuất cấp độ.

☐ Điều 12 Nghị định 85/2016/NĐ-CP.

Thành phần hồ sơ gửi thẩm định

1

Văn bản đề nghị thẩm định, phê duyệt HSDXCĐ theo Mẫu số 01 được ban hành kèm theo Nghị định số 85/2016/NĐ-CP (đối với HTTT đề xuất cấp độ 1 hoặc cấp độ 2) hoặc **Văn bản đề nghị thẩm định** HSDXCĐ theo Mẫu số 02 được ban hành kèm theo Nghị định số 85/2016/NĐ-CP (đối với HTTT 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 HTTT 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 căn cứ trên các tiêu chí theo quy định của pháp luật có đầy đủ các nội dung theo quy định tại khoản 4 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 các yêu cầu về kỹ thuật tương 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.

Thành phần hồ sơ gửi thẩm định (2)

3

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.

4

Tài liệu thiết kế hệ thống thông tin, là một trong những tài liệu sau:

- Đối với dự án đầu tư xây dựng mới hoặc mở rộng, nâng cấp HTTT: Thiết kế sơ bộ hoặc tài liệu có giá trị tương đương (Báo cáo kinh tế - kỹ thuật trong 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 trong trường hợp dự án đầu tư áp dụng phương án thiết kế 02 bước; Kế hoạch thuê dịch vụ công nghệ thông tin trong trường hợp áp dụng hình thức thuê dịch vụ CNTT hoặc Đề cương và dự toán chi tiết trong trường hợp đầu tư ứng dụng CNTT không phải lập dự án theo quy định);
- Đối với HTTT đang vận hành: Thiết kế thi công đã được cấp có thẩm quyền phê duyệt hoặc tài liệu có giá trị tương đương (Thiết kế chi tiết trong trường hợp dự án đầu tư; Kế hoạch thuê dịch vụ CNTT trong trường hợp áp dụng hình thức thuê dịch vụ CNTT; Đề cương và dự toán chi tiết trong trường hợp đầu tư ứng dụng CNTT không phải lập dự án theo quy định).

□ Điều 15 Nghị định số 85/2016/NĐ-CP và khoản 7 Điều 9 Thông tư số 12/2022/TT-BTTTT.

1

Hình thức thẩm định:

Tổ chức họp hoặc lấy ý kiến bằng văn bản hoặc áp dụng cả hai hình thức.

2

Nội dung thẩm định:

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:

- 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.

☐ Ý kiến thẩm định hồ sơ đề xuất cấp độ - Mẫu 04 Nghị định số 85/2016/NĐ-CP.



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:

- 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 (Khoản 2 Điều 6 Thông tư số 12/2022/TT-BTTTT);
- Chủ quản hệ thống thông tin ra Quyết định thành lập Hội đồng thẩm định.



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.

Về các thành viên Hội đồng thẩm định:

- 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;
- 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).

Hội đồng thẩm định độc lập (2)



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

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

- **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;
- **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** (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... công nghệ thông tin/an toàn thông tin có cấu phần) về kiến trúc 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** của Bộ trưởng Bộ Thông tin và Truyền thông.



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.

1,2

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

3

Đối với hệ thống thông tin được đề xuất cấp độ 3:

Theo quy định tại khoản 2 Điều 16 Nghị định số 85/2016/NĐ-CP, thời gian thẩm định tối đa là 15 ngày kể từ ngày nhận đủ hồ sơ hợp lệ.

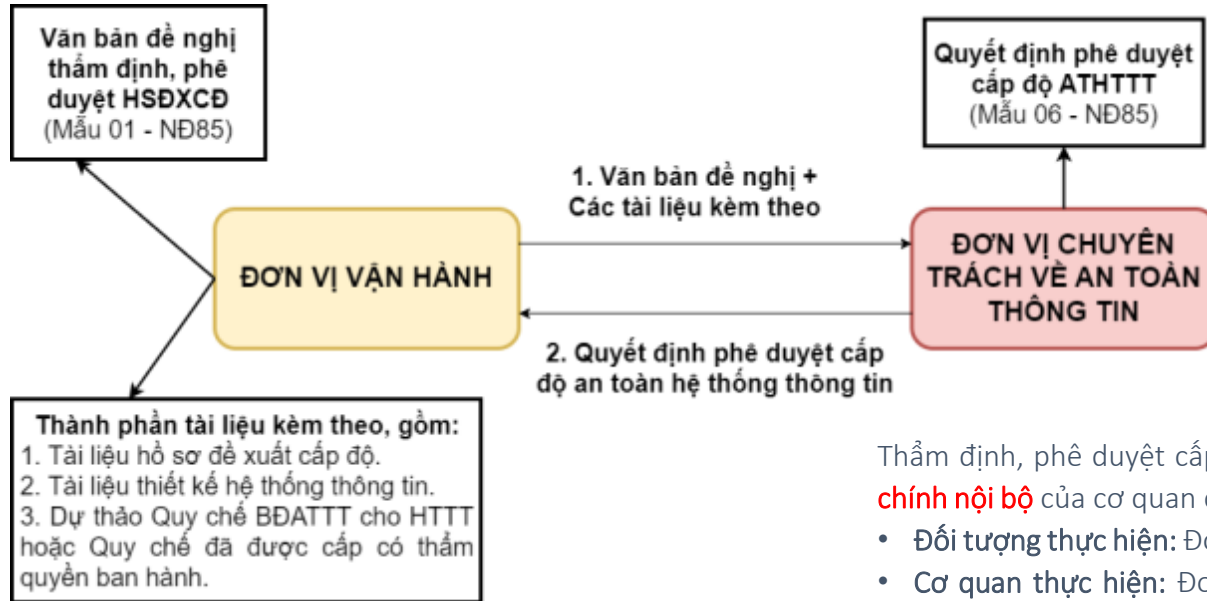
Thời gian phê duyệt: Tối đa 07 ngày làm việc kể từ ngày nhận đủ hồ sơ hợp lệ.



Lưu ý:

Trường hợp sau khi tổ chức thẩm định, HSĐXCĐ của HTTT 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.

Quy trình thẩm định, phê duyệt cấp độ 1, 2 | Trang 53/55



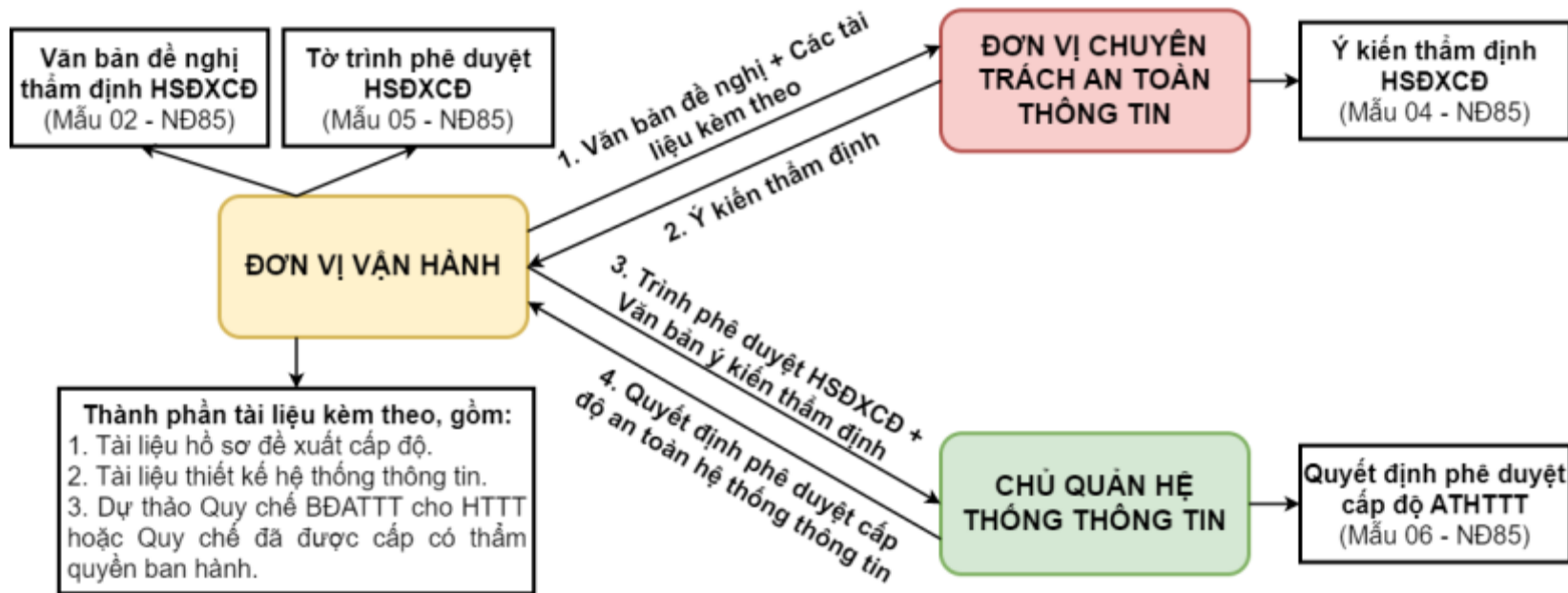
Thẩm định, phê duyệt cấp độ an toàn thông tin **được xem là thủ tục hành chính nội bộ** của cơ quan chủ quản hệ thống thông tin, trong đó:

- **Đối tượng thực hiện:** Đơn vị vận hành hệ thống thông tin;
- **Cơ quan thực hiện:** Đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin (đối với HTTT được đề xuất cấp độ 1 hoặc cấp độ 2) hoặc Chủ quản hệ thống thông tin (đối với HTTT được đề xuất cấp độ 3).

Lưu ý: Trước khi 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 đã phải được cấp có thẩm quyền phê duyệt, ban hành.

Quy trình thẩm định, phê duyệt cấp độ 3

Trang 54/55



Thời điểm phê duyệt HSDXCĐ



Thời điểm phê duyệt HSDXCĐ

Khuyến khích phê duyệt HSDXCĐ an toàn thông tin **trước khi cấp có thẩm quyền phê duyệt** Báo cáo kinh tế - kỹ thuật hoặc thiết kế cơ sở thuộc BCNCKT hoặc Kế hoạch thuê DVCNTT hoặc Đề cương và dự toán chi tiết tương ứng.



HTTT đang vận hành, khai thác, đã được phê duyệt cấp độ

Chủ quản hệ thống thông tin cần tiến hành rà soát HSDXCĐ và Phương án đảm bảo ATTT đã được phê duyệt, hoàn thành việc điều chỉnh, phê duyệt lại HSDXCĐ và Phương án bảo đảm ATTT (nếu cần) **trước 01/6/2023**.



CỤC AN TOÀN THÔNG TIN
AUTHORITY OF INFORMATION SECURITY

Năm 2023
Năm dữ liệu số quốc gia



GIẢI ĐÁP THẮC MẮC



CỤC AN TOÀN THÔNG TIN
AUTHORITY OF INFORMATION SECURITY

Năm 2023
Năm dữ liệu số quốc gia

TRÂN TRỌNG CẢM ƠN!

Chi tiết liên hệ: **Nguyễn Minh Dũng**

- ❖ Phòng An toàn hệ thống thông tin, Cục An toàn thông tin, Bộ Thông tin và Truyền thông;
- ❖ Điện thoại: 0914.646.840;
- ❖ Email: dungnm@mic.gov.vn.

