UBND TỈNH THANH HÓA
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số:2387/STTTT-CNTT&TT
V/v khẩn trương thực hiện phân loại, xác định và phê duyệt Hồ sơ đề xuất cấp độ an toàn hệ thống thông tin

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

Thanh Hoá, ngày 08 tháng 11 năm 2022

Kính gửi:
- Các Sở, ban, ngành, đơn vị cấp tỉnh;
- UBND các huyện, thị xã, thành phố;
- UBND các xã, phường, thị trấn.

Thực hiện Công văn số 15703/UBND-CNTT ngày 21/10/2022 của UBND tỉnh, về việc yêu cầu hoàn thành phân loại, xác định và phê duyệt Hồ sơ đề xuất cấp độ an toàn hệ thống thông tin, để bảo đảm hoàn thành phân loại, xác định và phê duyệt Hồ sơ đề xuất cấp độ an toàn hệ thống thông tin trên địa bàn tỉnh theo chỉ đạo của Chủ tịch UBND tỉnh; Sở Thông tin và Truyền thông hướng dẫn các cơ quan, đơn vị xác định cấp độ và lập hồ sơ đề xuất cấp độ an toàn hệ thống thông tin như sau:

1. Đối với các cơ quan, đơn vị đã được phê duyệt Hồ sơ đề xuất cấp độ (HSĐXCĐ).

- Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông về việc Quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ và Hướng dẫn của Sở Thông tin và Truyền thông tại Công văn số 2095/STTTT-CNTT ngày 03/10/2022; Các cơ quan, đơn vị thực hiện rà soát, điều chỉnh, phê duyệt lại Hồ sơ đề xuất cấp độ và Phương án bảo đảm an toàn thông tin.

- Tổ chức triển khai đầy đủ các phương án bảo đảm an toàn hệ thống thông tin theo cấp độ trước ngày 01/6/2023, gửi kết quả thực hiện về Sở Thông tin và Truyền thông trước ngày **15/5/2023** để tổng hợp báo cáo cấp có thẩm quyền theo quy định.

2. Đối với các cơ quan, đơn vị chưa thực hiện hoàn thành phê duyệt Hồ sơ đề xuất cấp độ.

- Các Sở, ban, ngành, đơn vị cấp tỉnh; UBND các huyện, thị xã, thành phố: tổ chức thực hiện phân loại, xác định cấp độ an toàn hệ thống thông tin đối với

các đơn vị trực thuộc, UBND cấp xã. Tổng hợp và gửi danh sách về Sở Thông tin và Truyền thông trước ngày **20/11/2022** theo mẫu tại Phụ lục 01 kèm theo.

- Tổ chức, triển khai xây dựng và trình phê duyệt Hồ sơ đề xuất cấp độ, gửi về Sở Thông tin và Truyền thông để thẩm định, trình cấp có thẩm quyền phê duyệt trước ngày **01/12/2022**.

- Tài liệu hướng dẫn xác định cấp độ, xây dựng Hồ sơ đề xuất cấp độ an toàn thông tin tại Phụ lục kèm theo, bao gồm:

+ Phụ lục 02: Hướng dẫn xác định cấp độ an toàn hệ thống thông tin

+ Phụ lục 03: Hướng dẫn xây dựng hồ sơ đề xuất cấp độ an toàn hệ thống thông tin.

Trong quá trình thực hiện, nếu có vướng mắc cần hỗ trợ, đề nghị các cơ quan, đơn vị phối hợp với Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa (thuộc Sở Thông tin và Truyền thông) để được hướng dẫn thực hiện.

Đầu mối liên hệ: Ông Trần Ngọc Hưng - Phó Giám đốc Trung tâm CNTT-TT Thanh Hóa, điện thoại: 0916.422583,

Thư điện tử: hungtn.ttcntt@thanhhoa.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Giám đốc Sở (để b/c);
- Trung tâm CNTT&TT Thanh Hóa (để t/h);
- Phòng QL CNTT (để p/h);
- Lưu: VT, CNTT&TT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH THANH HÓA

Nguyễn Văn Tước

PHỤ LỤC 01: Tổng hợp tình hình phân loại, xác định cấp độ an toàn hệ thống thông tin

(Kèm theo công văn số /STTTT-CNTT&TT ngày /11/2022 của Sở Thông tin và Truyền thông)

1. Thông tin chung

- Tổng số hệ thống thông tin thuộc phạm vi quản lý.
- Tổng số hệ thống thông tin đã được phân loại (đã xác định được loại hình hệ thống thông tin).
- Tổng số hệ thống thông tin đã xây dựng Hồ sơ đề xuất cấp độ.
- Tổng số Hồ sơ đề xuất cấp độ đã được thẩm định.
- Tổng số Hồ sơ đề xuất cấp độ đã được phê duyệt.

2. Thông tin chi tiết về các hệ thống thông tin

STT	Tên cơ quan, đơn vị	Tên hệ thống thông tin	Cấp độ đề xuất	Tình trạng phê duyệt HSĐXCĐ	Quyết định phê duyệt HSĐXCĐ
(1)	(2)	(3)	(4)	(5)	(6)
1					
2					

Chú thích:

- Cột (2): Ghi tên cơ quan, đơn vị
- Cột (3): Ghi tên hệ thống thông tin
- Cột (4): Ghi cấp độ đề xuất đối với hệ thống thông tin: Từ 1 đến 3.
- Cột (5): Ghi tình trạng phê duyệt hồ sơ đề xuất cấp độ (HSĐXCĐ) của hệ thống thông tin: Đang dự thảo; Đã gửi thẩm định; Đã thẩm định; Đã được phê duyệt.
- Cột (6): Ghi thông tin số, ngày Quyết định, tên cơ quan phê duyệt HSĐXCĐ nếu HSĐXCĐ đã được phê duyệt.

3. Thông tin đầu mối liên hệ

- Lãnh đạo cơ quan, đơn vị phụ trách chỉ đạo công tác tổ chức, đôn đốc xây dựng cấp độ an toàn hệ thống thông tin: Họ và tên, chức vụ, số điện thoại.
- Cán bộ xử lý trực tiếp: Bao gồm thông tin (họ và tên, chức vụ, số điện thoại) các cán bộ trực tiếp xây dựng HSĐXCĐ tại các cơ quan, đơn vị (*bao gồm các đơn vị trực thuộc, UBND cấp xã*) tại mục 2.

PHỤ LỤC 02: Hướng dẫn phân loại, xác định cấp độ an toàn hệ thống thông tin
(Kèm theo công văn số /STTTT-CNTT ngày //2022 của Sở Thông tin và Truyền thông)

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông về việc Quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ, Sở Thông tin và Truyền thông xây dựng hướng dẫn xác định độ an toàn hệ thống thông tin như sau:

1. Đối tượng áp dụng

Hướng dẫn áp dụng cho các sở, ban, ngành; Ủy ban nhân dân các huyện, thị xã, thành phố; Ủy ban nhân dân các xã, phường, thị trấn và các cơ quan, đơn vị có liên quan đến hoạt động xây dựng, thiết lập, quản lý, vận hành, nâng cấp, mở rộng hệ thống thông tin phục vụ ứng dụng công nghệ thông tin trong hoạt động của cơ quan, tổ chức nhà nước, ứng dụng công nghệ thông tin trong việc cung cấp dịch vụ trực tuyến phục vụ người dân và doanh nghiệp.

2. Giải thích từ ngữ

- 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.

- 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.

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

- Hệ thống 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.

- 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.

3. Tiêu chí phân loại, xác định cấp độ an toàn thông tin

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

3.1. 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.

3.2. Hệ thống thông tin cấp độ 2 là hệ thống thông tin có một trong các tiêu chí 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 người dân, doanh nghiệp thuộc một trong các loại hình như sau: (1) Cung cấp thông tin và dịch vụ công trực tuyến từ mức độ 2 trở xuống theo quy định của pháp luật; (2) Cung cấp dịch vụ trực tuyến không thuộc danh Mục dịch vụ kinh doanh có Điều kiện; (3) Cung cấp dịch vụ trực tuyến khác có xử lý thông tin riêng, thông tin cá nhân của dưới 10.000 người sử dụng.

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

3.3. Hệ thống thông tin cấp độ 3 là Hệ thống thông tin có một trong các tiêu chí 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 người dân, doanh nghiệp thuộc một trong các loại hình như sau: (1) Cung cấp thông tin và dịch vụ công trực tuyến từ mức độ 3 trở lên theo quy định của pháp luật; (2) Cung cấp dịch vụ trực tuyến thuộc danh mục dịch vụ kinh doanh có điều kiện; (3) 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.

- 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.

- 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.

**** Ví dụ một số hệ thống thông tin bảo đảm an toàn thông tin theo cấp độ:***

STT	Hệ thống thông tin	Cấp độ đề xuất	Căn cứ đề xuất
1	Hệ thống mạng nội bộ (LAN) xã A	1	Điều 7 Nghị định số 85/2016/NĐ-CP

2	Hệ thống hội nghị truyền hình trực tuyếnxã A	1	Điều 7 Nghị định số 85/2016/NĐ-CP
3	Trang thông tin điện tử của xã A	1	Điều 7 Nghị định số 85/2016/NĐ-CP

**** Lưu ý:***

- Trong quá trình phân loại, xác định cấp độ hệ thống thông tin. Cần thực hiện xác định rõ các thành phần của 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.

- Đối với cơ quan, đơn vị có nhiều hệ thống thông tin. Các hệ thống thông tin có cùng đơn vị Chủ quản, vận hành và dùng chung hạ tầng thì xây dựng thuyết minh trong 01 Hồ sơ đề xuất cấp độ. Nếu khác đơn vị chủ quản, vận hành và không dùng chung hạ tầng thì phải xây dựng thuyết minh độc lập với các Hồ sơ đề xuất cấp độ khác nhau.

**** Ví Dụ:***

- Trường hợp 1: *Sở A có Trung tâm B là đơn vị trực thuộc ở cùng một khuôn viên, sử dụng chung hệ thống thông tin thì chỉ xác định và xây dựng chung một hồ sơ đề xuất cấp độ cao nhất là Sở A*

-Trường hợp 2: *Sở A có Trung tâm B là đơn vị trực thuộc không cùng một khuôn viên thì phải xây dựng hồ sơ phê duyệt cấp độ cho từng cơ quan, đơn vị.*

-Trường hợp 3*: Xã A có 02 hệ thống thông tin bao gồm: (1) mạng nội bộ (2) trang thông tin điện tử. Trong đó trang thông tin điện tử thuê dịch vụ lưu trữ của đơn vị bên ngoài. Khi đó, Xã A phải xây dựng 02 thuyết minh hồ sơ cấp độ tương ứng với 02 hệ thống thông tin.*

4. Thẩm quyền, thành phần hồ sơ xác định cấp độ an toàn thông tin

4.1. Đối với hệ thống thông tin cấp độ 1 và cấp độ 2:

- Đơn vị đề xuất cấp độ an toàn hệ thống thông tin xây dựng hồ sơ theo Mẫu tại địa chỉ: *https://ais.gov.vn/thong-tin-tham-khao/mau-hsdxcd.htm*

- Văn bản gửi Sở Thông tin và Truyền thông tỉnh Thanh Hóa thẩm định và phê duyệt. Hồ sơ gồm: (1) Văn bản đề nghị thẩm định, phê duyệt đề xuất cấp độ theo Mẫu số 01 của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ; (2) Hồ sơ đề xuất cấp độ; (3) Quy chế bảo đảm an toàn hệ thống thông tin cho hệ thống được đề xuất đã được cấp có thẩm quyền phê duyệt, ban hành.

4.2. Đối với hệ thống thông tin cấp độ 3:

- Đơn vị đề xuất cấp độ an toàn hệ thống thông tin xây dựng hồ sơ theo Mẫu tại địa chỉ: *https://ais.gov.vn/thong-tin-tham-khao/mau-hsdxcd.htm*

- Đơn vị đề xuất cấp độ an toàn hệ thống thông tin gửi Văn bản đề nghị thẩm định hồ sơ đề xuất cấp độ theo Mẫu số 02 của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ.

- Tiếp thu ý kiến thẩm định của Sở Thông tin và Truyền thông tỉnh Thanh Hóa để điều chỉnh, hoàn thiện hồ sơ.

- Đơn vị đề xuất cấp độ an toàn hệ thống thông tin xây dựng Tờ trình theo Mẫu số 05 của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ trình Ủy ban nhân dân tỉnh phê duyệt. Hồ sơ đề xuất cấp độ an toàn hệ thống thông tin gồm: (1) Tờ trình phê duyệt đề xuất cấp độ; (2) Hồ sơ đề xuất cấp độ; (3) Quy chế bảo đảm an toàn hệ thống thông tin cho hệ thống được đề xuất đã được cấp có thẩm quyền phê duyệt, ban hành; (4) Văn bản thẩm định của Sở Thông tin và Truyền thông kết luận hệ thống thông tin của Đơn vị được thẩm định là phù hợp với cấp độ đề xuất.

**** Lưu ý:***

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

- Trong trường hợp thuê dịch vụ công nghệ thông tin đối với Hệ thống thông tin thì đơn vị vận hành hệ thống thông tin có trách nhiệm chủ trì, phối hợp với bên cung cấp dịch vụ xác định cấp độ và lập Hồ sơ đề xuất cấp độ an toàn thông tin; trình cấp thẩm quyền thẩm định và phê duyệt.

5. Điều khoản chuyển tiếp

- Đối với các hệ thống thông tin đang vận hành, khai thác, đã được phê duyệt cấp độ từ trước ngày Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông có hiệu lực: Chủ quản hệ thống thông tin tiến hành rà soát Hồ sơ đề xuất cấp độ và Phương án đảm bảo an toàn thông tin đã được phê duyệt. Việc rà soát, điều chỉnh, phê duyệt lại Hồ sơ đề xuất cấp độ và Phương án bảo đảm an toàn thông tin (nếu cần). Thực hiện trước tháng 6/2023.

- Đối với các hệ thống thông tin đang vận hành, khai thác nhưng chưa được phê duyệt Hồ sơ đề xuất cấp độ: Thực hiện xây dựng, thẩm định, phê duyệt Hồ sơ đề xuất cấp độ và triển khai phương án bảo đảm an toàn thông tin theo phương án đề xuất cấp độ đáp ứng các yêu cầu theo quy định tại Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông.

PHỤ LỤC 03: Hướng dẫn xây dựng hồ sơ đề xuất cấp độ an toàn hệ thống thông tin

(Kèm theo công văn số /STTTT-CNTT ngày //2022 của Sở Thông tin và Truyền thông)

Sở Thông tin và Truyền thông hướng dẫn mẫu xây dựng về hồ sơ phê duyệt cấp độ an toàn thông tin như sau:

***Trang bìa:** Bảo đảm đầy đủ các thông tin sau

CHỦ QUẢN HỆ THỐNG THÔNG TIN
ĐƠN VỊ VẬN HÀNH KHAI THÁC

HỒ SƠ ĐỀ XUẤT CẤP ĐỘ (1,2,3)
HỆ THỐNG THÔNG TIN A

Thanh Hóa - (Năm)

***Nội dung Hồ sơ:** Bảo đảm đầy đủ các thông tin sau

PHẦN I
THUYẾT MINH TỔNG QUAN VỀ HỆ THỐNG THÔNG TIN

1. Thông tin Chủ quản hệ thống thông tin

***Hướng dẫn**: Cung cấp thông tin về Chủ quản hệ thống thông tin căn cứ theo Điều 4,Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông, bao gồm các nội dung như ví dụ sau:*

- Tên Tổ chức: Cơ quan A.
- Số Quyết định thành lập/Quy định chức năng, nhiệm vụ và quyền hạn: Số 1234/QĐ…
- Người đại diện: Họ và tên, Chức vụ.

- Địa chỉ: Địa chỉ trụ sở cơ quan.

- Thông tin liên hệ: Số điện thoại, thư điện tử.

2. Thông tin Đơn vị vận hành

***Hướng dẫn**: Cung cấp thông tin về Đơn vị vận hành căn cứ theo Điều 5,Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông*

- Tên Đơn vị vận hành: Đơn vị B

- Số Quyết định thành lập/Quy định chức năng, nhiệm vụ và quyền hạn: Số 1234/QĐ…

- Người đại diện: Họ và tên, Chức vụ.

- Địa chỉ: Địa chỉ trụ sở của đơn vị.

- Thông tin liên hệ: Số điện thoại, thư điện tử.

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

***Hướng dẫn**: Làm rõ các nội dung (1) Phạm vi, quy mô của hệ thống; (2) Đối tượng phục vụ hệ thống (3) Danh mục các hệ thống thông tin thành phần/dịch vụ được cung cấp bởi hệ thống, bao gồm các nội như ví dụ sau:*

- Phạm vi, quy mô của hệ thống: Hệ thống thông tin A được được thiết lập để phục vụ công tác chỉ đạo điều hành, truy cập thông tin nội bộ và thông tin công cộng củacơ quan A.

- Đối tượng phục vụ của hệ thống: Cán bộ, công chức, người lao động của cơ quan A.

- Danh mục các hệ thống thông tin thành phần/các dịch vụ được cung cấp bởi Hệ thống:

+ Hệ thống mạng nội bộ (LAN)

+Hệ thống hội nghị truyền hình trực tuyến

4. Mô tả cấu trúc của hệ thống

Hướng dẫn xây dựng "Mô tả cấu trúc hiện tại của Hệ thống" gồm các mục:

(1) Mô hình Logic của hệ thống.

(2) Mô hình kết nối vật lý.

(3) 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 theo Mô hình vật lý của hệ thống.

(4) 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,

(5) 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).

PHẦN II
THUYẾT MINH CẤP ĐỘ ĐỀ XUẤT

1. Danh mục hệ thống thông tin và cấp độ đề xuất tương ứng

Hướng dẫn xây dựng "Danh mục hệ thống thông tin và cấp độ đề xuất tương ứng" gồm các mục: *(1) Tên hệ thống thông tin; (2) Cấp độ đề xuất; (3) Căn cứ đề xuất đối với từng hệ thống thông tin.*

- Trường hợp một hệ thống thông tin lớn, bao gồm nhiều thành phần khác nhau, thì cần xác định loại thông tin và loại hình của từng thành phần tương ứng. Thành phần nào có tiêu chí để đề xuất cấp độ cao nhất sẽ quyết định cấp
độ an toàn thông tin của hệ thống đó.

2. Thuyết minh đề xuất cấp độ đối với hệ thống thông tin

Hướng dẫn xây dựng "Thuyết minh đề xuất cấp độ đối với hệ thống thông tin" cần làm rõ các nội dung sau:

(1) Thông tin được xử lý.

(2) Loại hệ thống thông tin.

(3) Căn cứ đề xuất cấp độ đối với từng hệ thống.

PHẦN III
THUYẾT MINH PHƯƠNG ÁN
BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN

Hướng dẫn:

- Việc bảo đảm an toàn hệ thống thông tin theo cấp độ thực hiện theo yêu cầu cơ bản quy định tại Thông tư số 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017.

- 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.

Việc xây dựng phương án bảo đảm an toàn hệ thống thông tin gồm 02 nội dung chính về (1) Phương án đáp ứng yêu cầu cơ bản về quản lý; (2) Phương án đáp ứng yêu cầu cơ bản về kỹ thuật, đối với từng phương án cho mỗi cấp độ cụ thể như sau:

1. Phương án bảo đảm an toàn hệ thống thông tin cấp độ 1đáp ứng yêu cầu quy định chi tiết tại **Phụ lục I**của Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông:

1.1. Yêu cầu quản lý:

STT	Yêu cầu	TCVN 11930:2017
1.1	Thiết lập chính sách an toàn thông tin	Mục 5.1.1

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

1.2. Yêu cầu kỹ thuật

1.2.1. Yêu cầu về thiết kế hệ thống

a) Thiết kế các vùng mạng trong hệ thống theo chức năng, các vùng mạng tối thiểu bao gồm: (1) Vùng mạng nội bộ; (2) Vùng mạng biên; (3) Vùng DMZ.

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

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

STT	Yêu cầu	TCVN 11930:2017
1.1	**Bảo đảm an toàn mạng**	**Mục 5.2.1**
1.1.1	Kiểm soát truy cập từ bên ngoài mạng	Mục 5.2.1.2
1.1.2	Nhật kí hệ thống	Mục 5.2.1.3
1.1.3	Phòng chống xâm nhập	Mục 5.2.1.4
1.1.4	Bảo vệ thiết bị hệ thống	Mục 5.2.1.5
1.2	**Bảo đảm an toàn máy chủ**	**Mục 5.2.2**
1.2.1	Xác thực	Mục 5.2.2.1

1.2.2	Kiểm soát truy cập	Mục 5.2.2.2
1.2.3	Nhật ký hệ thống	Mục 5.2.2.3
1.2.4	Phòng chống xâm nhập	Mục 5.2.2.4
1.2.5	Phòng chống phần mềm độc hại	Mục 5.2.2.5
1.3	**Bảo đảm an toàn ứng dụng**	**Mục 5.2.3**
1.3.1	Xác thực	Mục 5.2.3.1
1.3.2	Kiểm soát truy cập	Mục 5.2.3.2
1.3.3	Nhật kí hệ thống	Mục 5.2.3.3
1.4	**Bảo đảm an toàn dữ liệu**	**Mục 5.2.4**
1.4.1	Sao lưu dự phòng	Mục 5.2.4.1

2. Phương án bảo đảm an toàn hệ thống thông tin cấp độ 2:đáp ứng yêu cầu quy định chi tiết tại Phụ lục II của Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông:

2.1. Yêu cầu quản lý

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

2.2. Yêu cầu kỹ thuật

2.2.1. Yêu cầu về thiết kế hệ thống

a) Thiết kế các vùng mạng trong hệ thống theo chức năng, các vùng mạng tối thiểu bao gồm: (1) Vùng mạng nội bộ; (2) Vùng mạng biên; (3) Vùng DMZ; (4) Vùng máy chủ nội bộ; (5) Vùng mạng không dây (nếu có) tách riêng, độc lập với các vùng mạng khác.

b) Có phương án thiết kế bảo đảm các yêu cầu sau: (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; (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; (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; (4) Có phương án phòng chống tấn công mạng cho ứng dụng web; sử dụng sản phẩm Tường lửa ứng dụng web đối với hệ thống thông tin theo quy định tại khoản 2 Điều 8 Nghị định 85/2016/NĐ-CP ; (5) Có phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử đối với hệ thống thư điện tử; (6) Có phương án dự phòng cho các thiết bị mạng chính, bao gồm thiết bị chuyển mạch trung tâm hoặc tương đương, thiết bị tường lửa trung tâm.

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

STT	Yêu cầu	TCVN 11930:2017
1.1	**Bảo đảm an toàn mạng**	**Mục 6.2.1**
1.1.1	Kiểm soát truy cập từ bên ngoài mạng	Mục 6.2.1.2
1.1.2	Kiểm soát truy cập từ bên trong mạng	Mục 6.2.1.3
1.1.3	Nhật kí hệ thống	Mục 6.2.1.4
1.1.4	Phòng chống xâm nhập	Mục 6.2.1.5
1.1.5	Bảo vệ thiết bị hệ thống	Mục 6.2.1.6
1.2	**Bảo đảm an toàn máy chủ**	**Mục 6.2.2**
1.2.1	Xác thực	Mục 6.2.2.1
1.2.2	Kiểm soát truy cập	Mục 6.2.2.2
1.2.3	Nhật ký hệ thống	Mục 6.2.2.3
1.2.4	Phòng chống xâm nhập	Mục 6.2.2.4
1.2.5	Phòng chống phần mềm độc hại	Mục 6.2.2.5
1.2.6	Xử lý máy chủ khi chuyển giao	Mục 6.2.2.6
1.3	**Bảo đảm an toàn ứng dụng**	**Mục 6.2.3**
1.3.1	Xác thực	Mục 6.2.3.1
1.3.2	Kiểm soát truy cập	Mục 6.2.3.2
1.3.3	Nhật kí hệ thống	Mục 6.2.3.3
1.3.4	An toàn ứng dụng và mã nguồn	Mục 6.2.3.4
1.4	**Bảo đảm an toàn dữ liệu**	**Mục 6.2.4**
1.4.1	Bảo mật dữ liệu	Mục 6.2.4.1
1.4.2	Sao lưu dự phòng	Mục 6.2.4.2

3. Phương án bảo đảm an toàn hệ thống thông tin cấp độ 3:đáp ứng yêu cầu quy định chi tiết tại Phụ lục III của Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông

3.1. Yêu cầu quản lý

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

3.2. Yêu cầu kỹ thuật

3.2.1. Yêu cầu về thiết kế hệ thống

a) Thiết kế các vùng mạng trong hệ thống theo chức năng, các vùng mạng tối thiểu bao gồm: (1) Vùng mạng nội bộ; (2) Vùng mạng biên; (3) Vùng DMZ; (4) Vùng máy chủ nội bộ; (5) Vùng mạng không dây (nếu có) tách riêng, độc lập với các vùng mạng khác; (6) Vùng mạng máy chủ cơ sở dữ liệu; (7) Vùng quản trị.

b) Có phương án thiết kế bảo đảm các yêu cầu sau: (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; 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 ; (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 sản phẩm Phòng, chống xâm nhập lớp mạng; (3) Có phương án cân bằng tải, dự phòng nóng cho các thiết bị mạng chính, tối thiểu bao gồm thiết bị chuyển mạch trung tâm hoặc tương đương, thiết bị tường lửa trung tâm, tường lửa ứng dụng web, hệ thống lưu trữ tập trung, tường lửa cơ sở dữ liệu (nếu có); (4) 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 ; (5) 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; (6) 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 ; (7) 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 ; (8) Có phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử; sử dụng sản phẩm Bảo đảm an toàn thông tin cho hệ thống thư điện tử đối với hệ thống Thư điện tử, đáp ứng tiêu chí quy định tại khoản 2 Điều 9 Nghị định 85/2016/NĐ-CP ; (9) 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 ; (10) Có phương án giám sát hệ thống thông tin tập trung; (11) 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; (12) 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; (13) 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; (14) 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 ; (15) Có phương án dự phòng kết nối mạng Internet cho các máy chủ dịch vụ; (16) Có phương án bảo đảm an toàn cho mạng không dây (nếu có).

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

STT	Yêu cầu	TCVN 11930:2017
1.1	**Bảo đảm an toàn mạng**	**Mục 7.2.1**
1.1.1	Kiểm soát truy cập từ bên ngoài mạng	Mục 7.2.1.2

1.1.2	Kiểm soát truy cập từ bên trong mạng	Mục 7.2.1.3
1.1.3	Nhật kí hệ thống	Mục 7.2.1.4
1.1.4	Phòng chống xâm nhập	Mục 7.2.1.5
1.1.5	Phòng chống phần mềm độc hại trên môi trường mạng	Mục 7.2.1.6
1.1.6	Bảo vệ thiết bị hệ thống	Mục 7.2.1.7
1.2	**Bảo đảm an toàn máy chủ**	**Mục 7.2.2**
1.2.1	Xác thực	Mục 7.2.2.1
1.2.2	Kiểm soát truy cập	Mục 7.2.2.2
1.2.3	Nhật ký hệ thống	Mục 7.2.2.3
1.2.4	Phòng chống xâm nhập	Mục 7.2.2.4
1.2.5	Phòng chống phần mềm độc hại	Mục 7.2.2.5
1.2.6	Xử lý máy chủ khi chuyển giao	Mục 7.2.2.6
1.3	**Bảo đảm an toàn ứng dụng**	**Mục 7.2.3**
1.3.1	Xác thực	Mục 7.2.3.1
1.3.2	Kiểm soát truy cập	Mục 7.2.3.2
1.3.3	Nhật kí hệ thống	Mục 7.2.3.3
1.3.4	Bảo mật thông tin liên lạc	Mục 7.2.3.4
1.3.5	Chống chối bỏ	Mục 7.2.3.5
1.3.6	An toàn ứng dụng và mã nguồn	Mục 7.2.3.6
1.4	**Bảo đảm an toàn dữ liệu**	**Mục 7.2.4**
1.4.1	Nguyên vẹn dữ liệu	Mục 7.2.4.1
1.4.2	Bảo mật dữ liệu	Mục 7.2.4.2
1.4.3	Sao lưu dự phòng	Mục 7.2.4.3