UBND TỈNH QUẢNG NGÃI **SỞ THÔNG TIN VÀ TRUYỀN THÔNG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 1119/STTTT-BCVT&CNTT V/v thực hiện cấp độ an toàn đối các với hệ thống thông tin	*Quảng Ngãi, ngày 22 tháng 6 năm 2023*

Kính gửi:
- Văn phòng UBND tỉnh;
- Các sở, ban, ngành; Hội đoàn thể tỉnh;
- UBND các huyện, thị xã, thành phố.

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

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

Căn cứ 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 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 Công văn số 713/CATTT-TĐQLGS ngày 25/7/2019 của Cục An toàn Thông tin - Bộ Thông tin và Truyền thông về việc hướng dẫn xác định và thực thi bảo vệ hệ thống thông tin;

Căn cứ Công văn số 822/CATTT-ATHTTT ngày 31/5/2023 của Cục An toàn Thông tin - Bộ Thông tin và Truyền thông về việc hướng dẫn công tác thẩm định và phê duyệt cấp độ an toàn hệ thống thông tin đối với cơ sở;

Thực hiện Kế hoạch số 166/KH-UBND ngày 14/10/2022 của UBND tỉnh Quảng Ngãi về Tăng cường đảm bảo an toàn, an ninh thông tin trong hoạt động các cơ quan nhà nước tỉnh Quảng Ngãi đến năm 2025 và định hướng đến năm 2030, Công văn số 1448/UBND-KGVX ngày 05/4/2023 về việc triển khai nhiệm vụ trọng tâm về an toàn thông tin mạng trong năm 2023 trên địa bàn tỉnhQuảng Ngãi. Thời gian qua, Sở Thông tin và Truyền thông đã ban hành nhiều văn bản[1] hướng dẫn các cơ quan, đơn vị, địa phương trong tỉnh lập hồ sơ phân loại, xác định cấp độ an toàn thông tin cho các hệ thống thông tin tại cơ quan, đơn vị. Nhằm thực hiện bảo vệ hệ thống thông tin theo quy định của pháp luật và hướng dẫn, tiêu chuẩn, quy chuẩn an toàn thông tin trong các cơ quan, đơn vị nhà nước đến cấp xã trên địa bàn tỉnh, Sở Thông tin và Truyền thông hướng đề nghị các cơ quan, đơn vị, địa phương triển khai một số nội dung, cụ thể như sau:

[1] Công văn số 994/STTTT ngày 20/9/2018 về việc Tổ chức phân loại, xác định cấp độ an toàn thông tin các hệ thống thông tin; Công văn số 445/STTTT ngày 04/5/2021 về việc hướng dẫn phân loại, xác định cấp độ an toàn thông tin của các hệ thống thông tin; Công văn số 1314/STTTT-BCVT&CNTT ngày 11/10/2021 về việc đôn đốc phân loại, xác định cấp độ an toàn thông tin của các hệ thống thông tin; Công văn số 438/STTTT-BCVT&CNTT ngày 12/04/2022 về việc đề nghị khẩn trương thực hiện phân loại, xác định cấp độ an toàn thông tin; 1800/STTTT-BCVT&CNTT ngày 05/12/2022 về phân loại, xác định cấp độ an toàn thông tin của các hệ thống thông tin.

1. Xác định và phân loại hệ thống thông tin; xác định đơn vị chủ quản hệ thống thông tin, đơn vị vận hành hệ thống thông tin theo quy định tại các Điều 5, 6 Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ và các Điều 4, 5, 6 Thông tư số 12/2022/TT-BTTTT ngày 12/ 8/ 2022 của Bộ trưởng Bộ Thông tin và Truyền thông.

2. Xác định loại thông tin được xử lý thông qua hệ thống thông tin theo quy định tại khoản 1 Điều 6 Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ.

3. Xác định cấp độ theo quy định tại Điều 7 đến Điều 11 Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ.

4. Về thẩm định, phê duyệt Hồ sơ cấp độ

a) Đối với Hồ sơ đề xuất cấp độ 1, 2: Các cơ quan, đơn vị chủ trì, phối hợp đơn vị liên quan xây dựng Hồ sơ đề xuất cấp độ gửi về đơn vị chuyên trách an toàn thông tin của chủ quản hệ thống.

- Đối với hệ thống thông tin của các sở, ban, ngành, UBND cấp huyện thì đơn vị chuyên trách an toàn thông tin của cơ quan chủ quản là Sở Thông tin và Truyền thông.

- Đối với hệ thống của các đơn vị trực thuộc sở, ban, ngành, UBND cấp huyện thì đơn vị chuyên trách an toàn thông tin là đơn vị thuộc sở, ban, ngành, UBND cấp huyện quản lý. ***Trường hợp chưa có đơn vị chuyên trách an toàn thông tin thì thực hiện theo điểm b Khoản 1 Điều 20 Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ.***

- Hồ sơ gồm:

+ Trường hợp nộp hồ sơ bản giấy, hồ sơ bao gồm: 01 bộ bản chính và 02 bộ bản sao hợp lệ

+ Trường hợp nộp hồ sơ bản điện tử, hồ sơ bao gồm: 01 bộ hồ sơ được ký số đầy đủ vào các nội dung thành phần.

b) Đối với Hồ sơ đề xuất cấp độ 3: Các cơ quan, đơn vị đang vận hành hệ thống chủ trì, phối hợp đơn vị liên quan xây dựng Hồ sơ đề xuất cấp độ gửi về Sở Thông tin và Truyền thông thẩm định; trình cơ quan chủ quản phê duyệt.

Hồ sơ gồm:

- Trường hợp nộp hồ sơ bản giấy, hồ sơ bao gồm: 01 bộ bản chính và 02 bộ bản sao hợp lệ

- Trường hợp nộp hồ sơ bản điện tử, hồ sơ bao gồm: 01 bộ hồ sơ được ký số đầy đủ vào các nội dung thành phần.

Ghi chú: Đối với các hồ sơ xuất cấp độ thuộc thẩm quyền thẩm định, phê duyệt của Sở Thông tin và Truyền thông, đề nghị gửi về Sở Thông tin và Truyền thông **trước ngày 30/8/2023**.

c) Đối với Hồ sơ đề xuất cấp độ 4, 5: Các cơ quan, đơn vị đang vận hành hệ thống chủ trì, phối hợp đơn vị liên quan xây dựng Hồ sơ đề xuất cấp độ gửi về Cục An toàn thông tin - Bộ Thông tin và Truyền thông để thẩm định; trình cơ

quan chủ quản phê duyệt. Hồ sơ gồm 01 bản chính và 04 bản sao hợp lệ.

5. Về triển khai phương án bảo đảm an toàn thông tin

Đơn vị vận hành hệ thống thông tin tổ chức triển khai phương án bảo đảm an toàn thông tin theo phương án thuyết minh trong Hồ sơ đề xuất cấp độ sau khi được phê duyệt và ban hành Phương án Ứng phó sự cố, bảo đảm an toàn thông tin đối với Hệ thống thông tin cảu đơn vị **(hoàn thành trước ngày 30/9/2023)**.

6. Đối với các đơn vị trực thuộc các sở, ban, ngành; các phòng chuyên môn trực thuộc UBND cấp huyện có sử dụng hệ thống mạng riêng *(nằm ngoài hệ thống mạng của các sở, ban, ngành; UBND cấp huyện)* và UBND cấp xã thực hiện xây dựng Hồ sơ đề xuất cấp độ và trình cấp có thẩm quyền thẩm định, phê duyệt cấp độ an toàn hệ thống thông tin ***trước ngày 30/8/2023***.

(Gửi kèm Tài liệu hướng dẫn xác định cấp độ an toàn thông tin tại Phụ lục kèm theo Công văn này)

Thông tin liên hệ hỗ trợ:

Ông Nguyễn Công Nguyên - Chuyên viên Phòng Bưu chính - Viễn thông và Công nghệ thông tin, Sở Thông tin và Truyền thông; điện thoại: 0914.559.068.

Đề nghị các cơ quan, đơn vị, địa phương triển khai thực hiện./.

Nơi nhận:
- Như trên;
- UBND tỉnh (báo cáo);
- Sở TT&TT: GĐ, PGĐ;
- Trung tâm CNTT&TT;
- Lưu: VT, BCVT&CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH QUẢNG NGÃI

Đỗ Quang Nghĩa

PHỤ LỤC I
QUY TRÌNH THỰC HIỆN XÁC ĐỊNH
CẤP ĐỘ AN TOÀN THÔNG TIN
(Kèm theo Công văn số / STTTT-BCVT&CNTTT ngày /6/2023 của Sở Thông tin và Truyền thông)

Quy trình thực hiện	Nội dung thực hiện	Kết quả/Ghi chú
Đối với hệ thống thông tin của các sở, ban, ngành, UBND cấp huyện		
Bước 1	Các sở, ban, ngành, UBND cấp huyện gửi hồ sơ đề xuất cấp độ an toàn hệ thống thông tin về Sở Thông tin và Truyền thông để thẩm định và phê duyệt cấp độ an toàn hệ thống thông tin	Hồ sơ gồm: 1. Tờ trình đề nghị thẩm định, phê duyệt Hồ sơ đề xuất cấp độ an toàn hệ thống thông tin; 2. Hồ sơ đề xuất cấp độ an toàn hệ thống thông tin.
Bước 2	Căn cứ hồ sơ của sở, ban, ngành, UBND cấp huyện, Sở Thông tin và Truyền thông sẽ tiến hành kiểm tra, thẩm định hồ sơ 1. Nếu hồ sơ đảm bảo yêu cầu, sẽ lập Báo cáo thẩm đinh. 2. Nếu hồ sơ không đạt yêu cầu sẽ đề nghị sở, ban, ngành, UBND cấp huyện giải trình, bổ sung.	Báo cáo thẩm định của Sở Thông tin và truyền thông
Bước 3	Sở Thông tin và Truyền thông ban hành Quyết định phê duyệt cấp độ an toàn hệ thống thông tin đối với hệ thống thông tin cấp độ 2	Quyết định phê duyệt cấp độ an toàn hệ thống thông tin đối với hệ thống thông tin cấp độ 2 *(Trường hợp hồ sơ đề xuất cấp độ 3 Sở Thông tin và Truyền thông sẽ trình UBND tỉnh xem xét phê duyệt)*
Đối với hệ thống thông tin của các cơ quan, đơn vị trực thuộc các sở, ban, ngành; các phòng chuyên môn, cơ quan, đơn vị trực thuộc UBND cấp huyện (bao gồm UBND các xã, phường, thị trấn)		
Bước 1	Các Sở, ban, ngành, UBND cấp huyện thành lập Tổ chuyên trách An toàn thông tin của đơn vị để tiến hành thẩm định hồ sơ. Hoặc chỉ định đơn vị chuyên trách về công nghệ thông tin làm nhiệm vụ đơn vị chuyên trách về an toàn thông tin	1. Quyết định thành lập Tổ chuyên trách An toàn thông tin của cở, ban, ngành, UBND cấp huyện.

Quy trình thực hiện	Nội dung thực hiện	Kết quả/Ghi chú
		2. Quyết định chỉ định chỉ định đơn vị chuyên trách về công nghệ thông tin làm nhiệm vụ đơn vị chuyên trách về an toàn thông tin
Bước 2	Các cơ quan, đơn vị trực thuộc các sở, ban, ngành, UBND cấp huyện gửi hồ sơ đề xuất cấp độ an toàn hệ thống thông tin về sở, ban, ngành, UBND cấp huyện *(qua đơn vị chuyên trách an toàn thông tin của sở, ban, ngành, UBND cấp huyện)*	Hồ sơ gồm: 1. Tờ trình đề nghị thẩm định, phê duyệt Hồ sơ đề xuất cấp độ an toàn hệ thống thông tin; 2. Hồ sơ đề xuất cấp độ an toàn hệ thống thông tin
Bước 3	Căn cứ hồ sơ của các cơ quan, đơn vị trực thuộc các sở, ban, ngành, UBND cấp huyện, Tổ chuyên trách An toàn thông tin hoặc đơn vị chuyên trách an toàn thông tin của đơn vị tiến hành kiểm tra, thẩm định hồ sơ 1. Nếu hồ sơ đảm bảo yêu cầu, sẽ lập Báo cáo thẩm đinh trình Giám đốc Sở ký ban hành. 2. Nếu hồ sơ không đạt yêu cầu đề nghị Các cơ quan, đơn vị trực thuộc các sở, ban, ngành, UBND cấp huyện giải trình, bổ sung.	Báo cáo thẩm định của Tổ chuyên trách An toàn thông tin hoặ đơn vị chuyên trách về an toàn thông tin của đơn vị
Bước 4	Sau khi nhận Báo cáo thẩm định của Tổ chuyên trách an toàn thông tin hoặc đơn vị chuyên trách an toàn thông tin của đơn vị; Các các sở, ban, ngành, UBND cấp huyện ban hành Quyết định phê duyệt cấp độ an toàn hệ thống thông tin.	Quyết định phê duyệt cấp độ an toàn hệ thống thông tin(cấp 1) của các sở, ban, ngành, UBND cấp huyện

PHỤ LỤC II
XÁC ĐỊNH CẤP ĐỘ AN TOÀN THÔNG TIN
(Kèm theo Công văn số / STTTT-BCVT&CNTTT ngày /6/2023 của Sở Thông tin và Truyền thông)

1. Xác định loại thông tin hệ thống thông tin xử lý

Một hệ thống thông tin có thể xử lý các loại thông tin dưới đây:

- 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.

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

Ví dụ: Hệ thống thông tin có xử lý thông tin bí mật nhà nước thì cấp độ tối thiểu là cấp độ 3. Hệ thống có xử lý thông tin riêng hoặc thông tin cá nhân thì cấp độ tối thiểu là cấp độ 2.

2. Xác định loại hình hệ thống thông tin

Hệ thống thông tin được phân loại theo chức năng phục vụ hoạt động nghiệp vụ như sau bao gồm 04 loại như sau:

(1) Hệ thống thông tin phục vụ hoạt động nội bộ là hệ thống chỉ phục vụ hoạt động quản trị, vận hành nội bộ của cơ quan, tổ chức. Bao gồm nhưng không giới hạn các hệ thống thông tin sau: Hệ thống thư điện tử; Hệ thống quản lý văn bản và điều hành; Hệ thống họp, hội nghị truyền hình trực tuyến; Hệ thống quản lý thông tin cụ thể (nhân sự, tài chính, tài sản hoặc lĩnh vực chuyên môn nghiệp vụ cụ thể khác) hoặc hệ thống quản lý thông tin tổng thể (tích hợp quản lý nhiều chức năng, nghiệp vụ khác nhau); Hệ thống xử lý thông tin nội bộ.

(2) Hệ thống thông tin phục vụ người dân, doanh nghiệp là hệ thống trực tiếp hoặc hỗ trợ cung cấp dịch vụ trực tuyến, bao gồm dịch vụ công trực tuyến và dịch vụ trực tuyến khác trong các lĩnh vực viễn thông, công nghệ thông tin, thương mại, tài chính, ngân hàng, y tế, giáo dục và các lĩnh vực chuyên ngành khác. Bao gồm nhưng không giới hạn các hệ thống thông tin sau: Hệ thống thư điện tử; Hệ thống quản lý văn bản và điều hành; Hệ thống một cửa điện tử; Hệ

thống trang, cổng thông tin điện tử; Hệ thống cung cấp hoặc hỗ trợ cung cấp dịch vụ trực tuyến; Hệ thống chăm sóc khách hàng.

(3) Hệ thống cơ sở hạ tầng thông tin là tập hợp trang thiết bị, đường truyền dẫn kết nối phục vụ hoạt động chung 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. Bao gồm nhưng không giới hạn các hệ thống thông tin sau: Mạng nội bộ, mạng diện rộng, mạng truyền số liệu chuyên dùng; Hệ thống cơ sở dữ liệu, trung tâm dữ liệu, điện toán đám mây; Hệ thống xác thực điện tử, chứng thực điện tử, chữ ký số; Hệ thống kết nối liên thông, trục tích hợp các hệ thống thông tin.

(4) Hệ thống thông tin điều khiển công nghiệp là hệ thống có chức năng giám sát, thu thập dữ liệu, quản lý và kiểm soát các hạng mục quan trọng phục vụ điều khiển, vận hành hoạt động bình thường của các công trình xây dựng. Bao gồm nhưng không giới hạn các hệ thống thông tin sau: Hệ thống điều khiển lập trình được (PLCs); Hệ thống điều khiển phân tán (DCS); Hệ thống giám sát và thu thập dữ liệu (SCADA).

Ngoài các hệ thống thông tin được phân loại ở trên thì còn có các hệ thống thông tin khác được sử dụng để trực tiếp phục vụ hoặc hỗ trợ hoạt động nghiệp vụ, sản xuất, kinh doanh cụ thể của cơ quan, tổ chức theo lĩnh vực chuyên ngành.

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

Tiêu chí xác định cấp độ an toàn hệ thống thông tin từ cấp độ 1 đến cấp độ 5 được quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ từ Điều 7 đến Điều 11.

Xác định cấp độ dựa vào các tiêu chí có thể được thực hiện theo các trường hợp sau:

- Trường hợp xác định cấp độ dựa vào thông tin mà hệ thống đó xử lý: Hệ thống thông tin cấp độ 1 chỉ xử lý thông tin công cộng. Hệ thống thông tin có xử lý thông tin riêng, thông tin cá nhân, cấp độ đề xuất tối thiểu là cấp độ 2; Hệ thống thông thông tin có xử lý thông tin bí mật nhà nước, cấp độ đề xuất tối thiểu là cấp độ 3.

- Trường hợp hệ thống thông tin là hệ thống cung cấp thông tin và dịch vụ công trực tuyến từ mức độ 2 trở xuống thì cấp độ đề xuất là cấp độ 2; Trường hợp hệ thống cung cấp thông tin và dịch vụ công trực tuyến từ mức độ 3 trở lên thì cấp độ là cấp độ 3.

- Trường hợp hệ thống thông tin cung cấp dịch vụ trực tuyến khác có xử lý thông tin riêng, thông tin cá nhân của dưới 10.000 người sử dụng thì cấp độ đề xuất là cấp độ 2; Trường hợp hệ thống cung cấp dịch vụ cho trên 10.000 người sử dụng thì cấp độ là cấp độ 3.

- Trường hợp hệ thống là 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 thì cấp độ đề xuất là cấp độ 3; Trường hợp phạm vi phục vụ trên phạm vi toàn quốc và yêu cầu vận hành 24/7 và không chấp nhận ngừng vận hành mà không có kế hoạch trước thì cấp độ đề xuất là cấp độ 4.

- Trường hợp hệ thống là hệ thống thông tin điều khiển công nghiệp trực tiếp phục vụ điều khiển, vận hành hoạt động bình thường của các công trình xây dựng cấp I theo phân cấp của pháp luật về xây dựng thì cấp độ đề xuất là cấp độ 4; Trường hợp hệ thống phục vụ điều khiển công trình xây dựng cấp đặc biệt theo phân cấp của pháp luật về xây dựng hoặc công trình quan trọng liên quan đến an ninh quốc gia theo pháp luật về an ninh quốc gia thì cấp độ đề xuất là cấp độ 5.

Đối với các trường hợp khác, việc xác định cấp độ an toàn thông tin căn cứ vào các quy định tại Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ và Thông tư số 12/2022/TT-BTTTT ngày 12/8/ 2022 của Bộ trưởng Bộ Thông tin và Truyền thông.

PHỤ LỤC III
XÂY DỰNG HỒ SƠ CẤP ĐỘ, THAM KHẢO MẪU HỒ SƠ VÀ MẪU VĂN BẢN XÁC ĐỊNH CẤP ĐỘ AN TOÀN HỆ THỐNG THÔNG TIN

(Kèm theo Công văn số /STTTT-BCVT&CNTT ngày /6/2023 của Sở Thông tin và Truyền thông)

PHẦN A. XÂY DỰNG HỒ SƠ CẤP ĐỘ AN TOÀN THÔNG TIN

I. Hồ sơ đề xuất cấp độ bao gồm:

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

2. Tài liệu thiết kế là một trong những tài liệu sau:

a) Đối với dự án đầu tư xây dựng mới hoặc mở rộng, nâng cấp hệ thống thông tin: Thiết kế sơ bộ hoặc tài liệu có giá trị tương đương;

b) Đối với hệ thống thông tin đang vận hành: 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.

II. Yêu cầu cơ bản đối với từng cấp độ

1. Phương án bảo đảm an toàn hệ thống thông tin **cấp độ 1** phải đáp ứng yêu cầu quy định chi tiết tại **Mẫu số 01** ban hành kèm theo Công văn này.

2. Phương án bảo đảm an toàn hệ thống thông tin **cấp độ 2** phải đáp ứng yêu cầu như đối với cấp độ 1 và bổ sung yêu cầu quy định chi tiết tại **Mẫu số 02** ban hành kèm theo Công văn này.

3. Phương án bảo đảm an toàn hệ thống thông tin **cấp độ 3** phải đáp ứng yêu cầu như đối với cấp độ 2 và bổ sung yêu cầu quy định chi tiết tại **Mẫu số 03** ban hành kèm theo Công văn này.

4. Phương án bảo đảm an toàn hệ thống thông tin **cấp độ 4** phải đáp ứng yêu cầu như đối với cấp độ 3 và bổ sung yêu cầu quy định chi tiết tại **Mẫu số 04** ban hành kèm theo Công văn này.

5. Phương án bảo đảm an toàn hệ thống thông tin **cấp độ 5** phải đáp ứng yêu cầu như đối với cấp độ 4 và bổ sung yêu cầu quy định chi tiết tại **Mẫu số 05** ban hành kèm theo Công văn này.

Mẫu số 01
YÊU CẦU CƠ BẢN BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN ĐỐI VỚI HỆ THỐNG THÔNG TIN CẤP ĐỘ 1

1. Yêu cầu kỹ thuật:

a) An toàn máy chủ:

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

- Không sử dụng kết nối không được mã hóa trong việc quản trị máy chủ từ xa;

b) An toàn ứng dụng:

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

c) An toàn dữ liệu:

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

2. Yêu cầu quản lý:

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

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

Mẫu số 02
YÊU CẦU CƠ BẢN BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN ĐỐI VỚI HỆ THỐNG THÔNG TIN CẤP ĐỘ 2

1. Yêu cầu kỹ thuật:

a) An toàn hạ tầng mạng:

- Có phân vùng hạ tầng mạng thành các vùng mạng khác nhau tùy theo yêu cầu, mục đích sử dụng;

- Có phương án sử dụng thiết bị có chức năng tường lửa để ngăn chặn truy cập trái phép giữa các vùng mạng với mạng Internet;

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

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

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

b) An toàn máy chủ:

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

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

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

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

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

c) An toàn ứng dụng:

- Có thiết lập yêu cầu bảo đảm mật khẩu trên ứng dụng đủ độ phức tạp cần thiết để hạn chế tấn công dò quét mật khẩu; các thông tin xác thực phải được lưu trữ dưới dạng mã hóa;

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

- Không sử dụng kết nối mạng không mã hóa trong việc quản trị ứng dụng từ xa.

d) An toàn dữ liệu: Có phương án sử dụng hệ thống hoặc phương tiện lưu

trữ độc lập để sao lưu dự phòng các dữ liệu quan trọng trên máy chủ. Việc sao lưu được thực hiện định kỳ theo quy định của tổ chức.

2. Yêu cầu quản lý:

a) Chính sách chung:

- Có chính sách an toàn thông tin cho người sử dụng bao gồm các nội dung: chính sách truy cập và sử dụng mạng và tài nguyên trên Internet; truy cập và sử dụng ứng dụng;

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

b) Tổ chức, nhân sự:

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

c) Quản lý thiết kế, xây dựng:

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

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

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

d) Quản lý vận hành:

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

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

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

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

- Việc kiểm tra, đánh giá an toàn thông tin và đánh giá rủi ro phải do đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin thực hiện hoặc thuê ngoài thực hiện theo quy định của pháp luật.

Mẫu số 03
YÊU CẦU CƠ BẢN BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN ĐỐI VỚI HỆ THỐNG THÔNG TIN CẤP ĐỘ 3

1. Yêu cầu kỹ thuật:

a) An toàn hạ tầng mạng:

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

- Có thiết kế vùng mạng nội bộ thành các mạng chức năng riêng theo yêu cầu nghiệp vụ; phân vùng mạng riêng cho mạng không dây tách biệt với các vùng mạng chức năng; phân vùng mạng riêng cho các máy chủ cung cấp dịch vụ ra ngoài mạng Internet;

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

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

- Có phương án sử dụng thiết bị có chức năng tường lửa giữa các vùng mạng quan trọng;

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

- Có lưu trữ nhật ký các thiết bị mạng và quản lý tập trung trong vùng mạng quản trị đối với các thiết bị mạng có hỗ trợ tính năng này hoặc thiết bị mạng quan trọng;

- Có lưu trữ tối thiểu trong 03 tháng đối với nhật ký của các thiết bị mạng và bảo đảm đồng bộ thời gian nhật ký với máy chủ thời gian thực theo múi giờ Việt Nam;

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

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

- Có phương án xác thực tài khoản quản trị trên tất cả các thiết bị mạng trong đó bảo đảm yêu cầu về mật khẩu có độ phức tạp cần thiết, phòng chống dò quét mật khẩu;

- Có phương án giới hạn các nguồn truy cập, quản trị các thiết bị mạng;

- Có phương án chỉ cho phép quản trị các thiết bị mạng thông qua mạng Internet bằng mạng riêng ảo hoặc các phương pháp khác tương đương;

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

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

b) An toàn máy chủ:

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

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

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

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

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

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

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

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

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

c) An toàn ứng dụng:

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

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

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

- Có phương án kiểm tra, lọc các dữ liệu đầu vào từ phía người sử dụng, bảo đảm các dữ liệu này không ảnh hưởng đến an toàn thông tin của ứng dụng.

d) An toàn dữ liệu:

- Có phương án mã hóa dữ liệu lưu trữ (không phải là thông tin, dữ liệu

công khai) trên hệ thống lưu trữ/phương tiện lưu trữ;

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

2. Yêu cầu quản lý:

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

b) Tổ chức, nhân sự:

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

- Có chính sách yêu cầu cán bộ liên quan khi thôi việc cần cam kết giữ bí mật thông tin liên quan đến dữ liệu trên hệ thống, thông tin riêng của tổ chức hoặc thông tin nhạy cảm khác;

c) Thiết kế, xây dựng hệ thống:

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

d) Quản lý vận hành:

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

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

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

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

- Định kỳ hàng năm thực hiện kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin theo quy định của pháp luật;

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

Mẫu số 04
YÊU CẦU CƠ BẢN BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN ĐỐI VỚI HỆ THỐNG THÔNG TIN CẤP ĐỘ 4

1. Yêu cầu về kỹ thuật:

a) An toàn hạ tầng mạng:

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

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

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

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

- Có phương án sử dụng thêm các phương pháp xác thực đa nhân tố đối với các thiết bị mạng quan trọng;

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

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

- Có phương án duy trì ít nhất 02 kết nối mạng Internet từ các ISP sử dụng hạ tầng kết nối trong nước khác nhau (nếu hệ thống buộc phải có kết nối mạng Internet);

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

b) An toàn máy chủ:

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

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

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

c) An toàn ứng dụng:

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

tin xác thực định kỳ;

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

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

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

d) An toàn dữ liệu:

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

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

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

2. Yêu cầu quản lý:

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

b) Tổ chức, nhân sự:

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

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

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

c) Thiết kế, xây dựng hệ thống:

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

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

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

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

d) Quản lý vận hành:

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

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

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

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

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

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

Mẫu số 05
YÊU CẦU CƠ BẢN BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN ĐỐI VỚI HỆ THỐNG THÔNG TIN CẤP ĐỘ 5

1. Yêu cầu kỹ thuật:

a) An toàn hạ tầng mạng:

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

- Có phương án lưu dữ liệu nhật ký của các thiết bị mạng tối thiểu 12 tháng;

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

b) An toàn máy chủ:

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

- Có phương án lưu trữ nhật ký độc lập và phù hợp với hoạt động của máy chủ. Nhật ký của hệ thống phải được lưu tối thiểu 12 tháng;

c) An toàn ứng dụng:

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

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

- Có phương án lưu nhật ký của ứng dụng lưu tối thiểu 12 tháng;

d) An toàn dữ liệu:

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

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

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

2. Yêu cầu quản lý:

a) Chính sách chung:

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

b) Chính sách tổ chức, nhân sự:

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

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

c) Thiết kế, xây dựng hệ thống:

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

d) Quản lý vận hành:

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

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

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

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

PHẦN B: MẪU HỒ SƠ THAM KHẢO ĐỀ XUẤT CẤP ĐỘ AN TOÀN HỆ THỐNG THÔNG TIN

1. Tài liệu thuyết minh Hồ sơ đề xuất cấp độ bao gồm các nội dung:

a) Mô tả, thuyết minh tổng quan về hệ thống thông tin.

b) Thuyết minh về việc đề xuất cấp độ căn cứ trên các tiêu chí theo quy định của pháp luật.

c) Thuyết minh phương án bảo đảm an toàn thông tin theo cấp độ tương ứng.

2. Tài liệu thiết kế hệ thống là một trong những tài liệu sau:

a) Đối với dự án đầu tư xây dựng mới hoặc mở rộng, nâng cấp hệ thống thông tin: Thiết kế sơ bộ hoặc tài liệu có giá trị tương đương;

b) Đối với hệ thống thông tin đang vận hành: Thiết kế thi công đã được cấp có thẩm quyền phê duyệt hoặc tài liệu có giá trị tương đương.

Khi xây dựng Hồ sơ đề xuất cấp độ cần chú ý, đối với một hệ thống thông tin lớn có nhiều hệ thống thành phần, trong đó, các hệ thống thành phần được quản lý, chia sẻ trên một hạ tầng dùng chung, có cùng đơn vị vận hành và có thể triển khai phương án bảo đảm an toàn thông tin chung cho toàn bộ hạ tầng đó, thì có thể xây dựng một Hồ sơ đề xuất cấp độ chung cho các hệ thống thông tin thành phần. Chỉ xây dựng Hồ sơ đề xuất cấp độ riêng biệt trong trường hợp độc lập về hạ tầng, cơ chế quản lý và đơn vị vận hành.

Xây dựng Hồ sơ đề xuất cấp độ theo hướng dẫn mẫu sau:

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

(MẪU)
TÀI LIỆU THUYẾT MINH HỒ SƠ ĐỀ XUẤT CẤP ĐỘ CHO HỆ THỐNG THÔNG TIN A

Quảng Ngãi, năm ...

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, bao gồm:*

- Tên Tổ chức: (Ví dụ) Cơ quan A.

- Số Quyết định thành lập/Quy định chức năng, nhiệm vụ và quyền hạn.

- 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, bao gồm:*

- Tên Đơn vị vận hành: (Ví dụ) Đơn vị AA.

- Số Quyết định thành lập/Quy định chức năng, nhiệm vụ và quyền hạn.

- 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.

Trường hợp hệ thống thông tin lớn có nhiều đơn vị vận hành khác nhau thì cung cấp đầy đủ thông tin của các đơn vị vận hành.

3. Mô tả phạm vi, quy mô của hệ thống

Hướng dẫn:** Mô tả phạm vi, quy mô, thành phần các ứng dụng, dịch vụ và đối tượng cung cấp dịch vụ của Hệ thống. Chú ý là một hệ thống thông tin có thể bao gồm nhiều hệ thống thông tin thành phần và mỗi thành phần trong đó có thể cung cấp một ứng dụng, dịch vụ khác nhau. **Ví dụ:

- Phạm vi, quy mô của hệ thống: Hệ thống thông tin A được thiết lập để phục vụ công tác chỉ đạo điều hành, cung cấp thông tin và cung cấp dịch vụ công trực tuyến của tỉnh/cơ quan A.

- Đối tượng phục vụ của hệ thống: Cơ quan, tổ chức, doanh nghiệp, người dẫn trên địa bàn tỉnh/cơ quan A.

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

+ Hệ thống quản lý văn bản và điều hành.

+ Hệ thống thông tin một cửa điện tử.

+ Hệ thống cổng thông tin điện tử.

+ Hệ thống thư điện tử công vụ.

+ Hệ thống báo cáo trực tuyến và thông tin KT-XH.

+ Hệ thống quản lý hồ sơ CBCCVC và đánh giá kết quả làm việc.

+ Hệ thống quản lý công tác thanh tra…

4. Mô tả cấu trúc của hệ thống

***Hướng dẫn**: Mô tả cấu trúc hiện tại của Hệ thống, bao gồm các thông tin:*

a) Cấu trúc logic mô tả thiết kế các vùng mạng chức năng có trong hệ thống; hướng kết nối mạng; các thiết bị đầu cuối; các thiết bị mạng. Trường hợp các thiết bị vật lý được cài đặt các thành phần ảo hóa hoặc logic, hoạt động như một thiết bị độc lập thì sơ đồ logic sẽ thể hiện thành phần ảo hóa hoặc logic thay cho thiết bị vật lý.

Trường hợp các hệ thống thông tin có cấu trúc đặt thù theo chức năng và không có những vùng mạng được đưa ra như trong Thông tư số 12/2022/TT-BTTTT ngày 12/ 8/ 2022 của Bộ trưởng Bộ Thông tin và Truyền thông về quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ (gọi tắt là Thông tư 12) thì việc mô tả cấu trúc của hệ thống thông tin đó được mô tả theo cấu trúc thực tế của hệ thống.

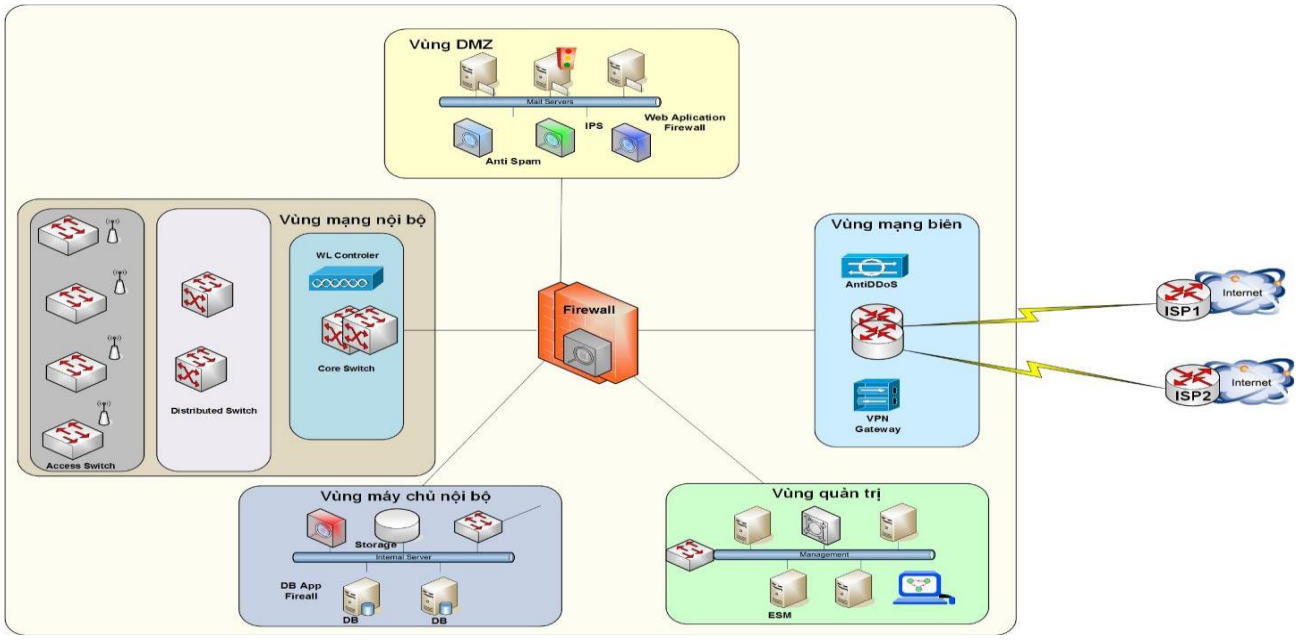
b) Cấu trúc vật lý mô tả các thiết bị mạng, các thiết bị đầu cuối có trong hệ thống và các kết nối vật lý giữa các thiết bị.

c) Cung cấp danh mục thiết bị sử dụng trong hệ thống: Cung cấp thông tin về các thiết bị mạng và các thiết bị đầu cuối có trong hệ thống. Bao gồm các thông tin Tên thiết bị/Chủng loại; Vị trí triển khai, trường hợp thiết bị vật lý được chia thành các thiết bị logic thì vị trí triển khai là các vị trí của thiết bị logic.

d) Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống (bao gồm các ứng dụng nghiệp vụ như quản lý văn bản, thư điện tử… và các dịch vụ hệ thống như DNS, DHCP, NTP…) : Cung cấp thông tin các ứng dụng/dịch vụ có trên 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.

Ví dụ 1: Mô tả cấu trúc hệ thống đối với Hệ thống A như sau:

a) Sơ đồ logic tổng thể



Hình 1: Cấu trúc logic của hệ thống A

Các vùng mạng được thiết kế như sau:

+ Vùng mạng biên được thiết kế để kết nối hệ thống mạng A ra các mạng bên ngoài và mạng Internet; bảo vệ hệ thống A từ bên ngoài Internet. Vùng mạng này triển khai hệ thống phòng chống tấn công DDoS và Thiết bị cung cấp cổng kết nối VPN.

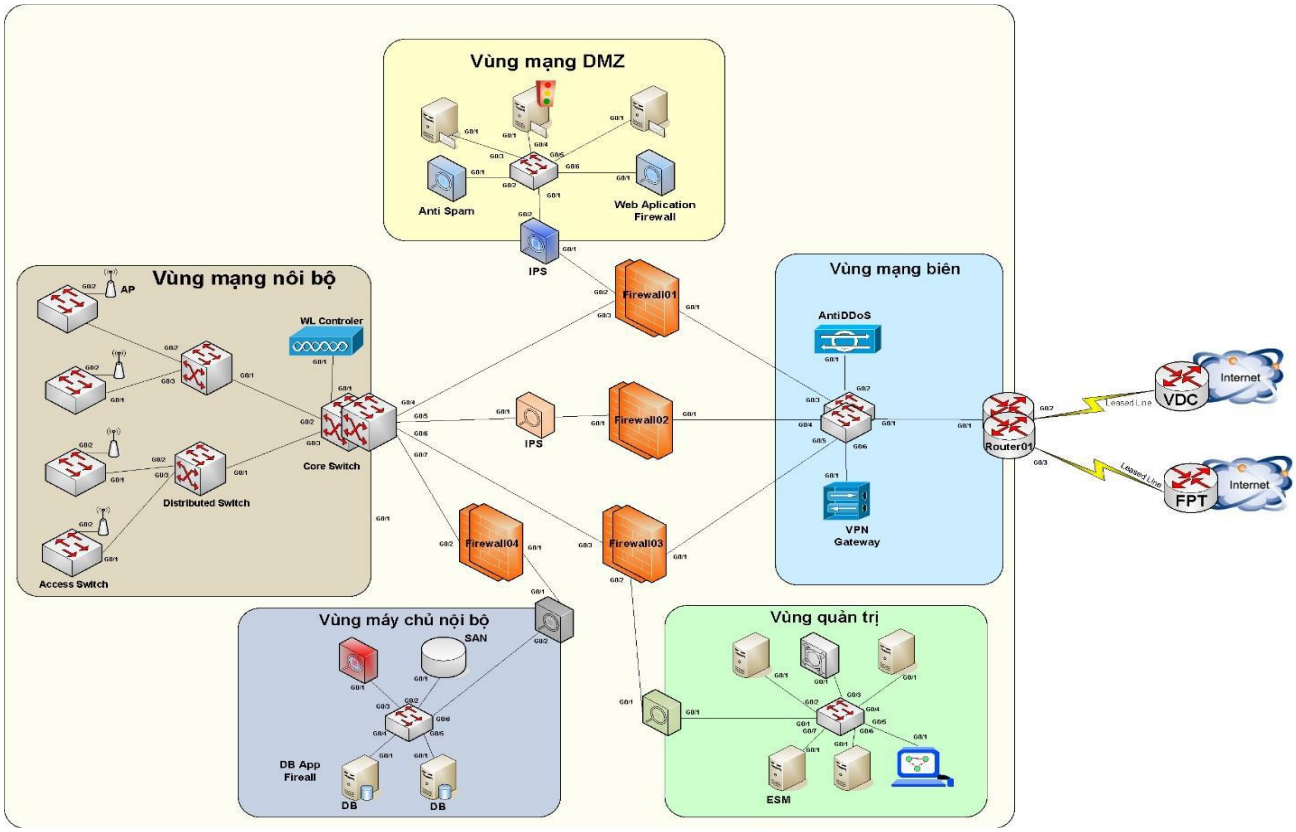
+ Vùng DMZ đặt các máy chủ công cộng, cung cấp dịch vụ ra bên ngoài Internet. Vùng mạng này triển khai thiết bị phòng chống xâm nhập IPS, thiết bị Web Application Firewall, thiết bị Anti-Spam.

+ Vùng mạng quản trị đặt các máy chủ quản trị và máy chủ hệ thống.

+ Vùng máy chủ nội bộ đặt các máy chủ nội bộ, cung cấp các dịch vụ nội bộ cho người sử dụng trong hệ thống. Vùng mạng này triển khai thiết bị phòng chống xâm nhập IPS, thiết bị Web Application Firewall, thiết bị tường lửa cho CSDL…

+ Vùng mạng nội bộ đặt các máy tính của người sử dụng.

b) Sơ đồ kết nối vật lý



Hình 2: Kết nối vật lý của Hệ thống A

c) Danh mục thiết bị sử dụng trong hệ thống

STT	Tên thiết bị/Chủng loại	Vị trí triển khai	Mục đích sử dụng
1	Router01/Cisco3800	Vùng mạng biên	Kết nối và định tuyến động với các Router của 02 ISP
2	Firewall01/ASA 5505	Vùng DMZ	Quản lý truy cập và bảo vệ vùng mạng DMZ
3	…	…	….

d) Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống

STT	Tên dịch vụ	Máy chủ triển khai	Mục đích sử dụng
1	Hệ thống quản lý văn bản và điều hành	Máy chủ Noibo01/ Vùng máy chủ nội bộ/ WindowServer 2012	Cung cấp ứng dụng quản lý văn bản cho cán bộ bên trong hệ thống; kết nối, liên thông với các hệ thống liên quan
2	Hệ thống thông tin một cửa điện	Máy chủ Noibo02/ Vùng máy chủ nội	Cung cấp ứng dụng theo dõi, quản lý thông tin tiếp nhận,

	tử	bộ/ Centos7	giải quyết TTHC bên trong hệ thống và cung cấp thông tin công khai về DVCTT, tình trạng giải quyết TTHC cho người sử dụng bên ngoài Internet
3	…	…	…

PHẦN II
THUYẾT MINH ĐỀ XUẤT CẤP ĐỘ AN TOÀN HỆ THỐNG THÔNG TIN

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

Hướng dẫn: Việc xác định cấp độ của hệ thống thông tin căn cứ vào loại thông tin hệ thống đó xử lý và loại hình hệ thống thông tin đó.

Khi xác định cấp độ, ta không cần thiết phải liệt kê ra hết các tiêu chí, mà chỉ đưa ra duy nhất một tiêu chí và tiêu chí đó đủ để xác định cấp độ cao nhất.

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. Do đó, khi xác định cấp độ của Hệ thống thông tin cần xác định thành phần nào trong hệ thống thông tin tổng thể khớp với tiêu chí xác định cấp độ ở cấp cao nhất.

Thành phần của hệ thống thông tin có thể phân chia bằng nhiều hình thức khác nhau, miễn là ta có thể phân biệt được thành phần đó với các thành phần khác trong hệ thống theo cách phân chia được thực hiện.

Thành phần của hệ thống có thể phân theo các **ứng dụng/dịch vụ** cụ thể (Thư điện tử, Cổng thông tin điện tử…) hoặc phân theo **vùng mạng** (Vùng DMZ, Vùng máy chủ nội bộ,…) hay **chức năng** (Hệ thống chăm sóc khác hàng, hệ thống truyền hình trực tuyến…) của thành phần đó.

Khi các thành phần trong hệ thống được phân chia theo các ứng dụng/dịch vụ và được quy hoạch vào một vùng mạng thì ứng dụng/dịch vụ nào quan trọng nhất sẽ quyết định tiêu chí xác định cấp độ của vùng mạng đó.

Chú ý: Việc phân chia hệ thống thông tin thành các thành phần cần phải đảm bảo số lượng các thành phần là nhỏ, đơn giản nhất và đủ để áp dụng các tiêu chí để xác định cấp độ cho hệ thống thông tin đó.

Ví dụ: Hệ thống thông tin thuộc phạm vi quản lý của cơ quan A bao gồm các hệ thống thông tin với cấp độ đề xuất tương ứng, bao gồm:

STT	Hệ thống	Loại thông tin xử lý	Loại hình HTTT	Cấp độ đề xuất	Căn cứ đề xuất
1	Phòng máy chủ/Trung tâm tích hợp dữ liệu của tỉnh		Hệ thống cơ sở hạ tầng thông tin dùng chung phục vụ hoạt động của các cơ quan,	3	Khoản 3, Điều 9 Nghị định số 85/2016/NĐ-CP

			tổ chức trong phạm vi ngành/tỉnh		
2	Hệ thống quản lý văn bản và điều hành của tỉnh	Thông tin riêng	Hệ thống thông tin phục vụ hoạt động nội bộ các cơ quan nhà nước của tỉnh	2	Khoản 1, Điều 8 Nghị định số 85/2016/NĐ-CP
3	Hệ thống một cửa điện tử của tỉnh	Thông tin công cộng, thông tin riêng và thông tin cá nhân	Hệ thống thông tin phục vụ người dân, doanh nghiệp	3	Khoản 2, Điều 9 Nghị định số 85/2016/NĐ-CP
4	Cổng thông tin điện tử của tỉnh	Thông tin công cộng	Hệ thống thông tin phục vụ người dân, doanh nghiệp, cung cấp thông tin và DVC trực tuyến từ mức độ 2 trở xuống	2	Điểm a, Khoản 2, Điều 8 Nghị định số 85/2016/NĐ-CP
5	Hệ thống thư điện tử công vụ của tỉnh	Thông tin riêng	Hệ thống thông tin phục vụ hoạt động nội bộ các cơ quan nhà nước của tỉnh kết hợp cung cấp dịch vụ trực tuyến có xử lý thông tin riêng dưới 10.000 người sử dụng	2	Điểm c, Khoản 2, Điều 8 Nghị định số 85/2016/NĐ-CP
6	Hệ thống quản lý hồ sơ CBCCVC và đánh giá kết quả làm việc của tỉnh	Thông tin riêng	Hệ thống thông tin phục vụ hoạt động nội bộ các cơ	2	Khoản 1, Điều 8 Nghị định số 85/2016/NĐ-CP

			quan nhà nước của tỉnh		
7	Hệ thống mạng nội bộ - LAN của cơ quan		Hệ thống cơ sở hạ tầng thông tin phục vụ hoạt động của cơ quan	2	Khoản 3, Điều 8 Nghị định số 85/2016/NĐ-CP
8	…				

2. Thuyết minh chi tiết đối với hệ thống thông tin

Hướng dẫn: Nội dung này chỉ yêu cầu đối với hệ thống được đề xuất là **cấp độ 4 hoặc cấp độ 5**, theo khoản 4, Điều 7 Thông tư 12. Bao gồm các nội dung:

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; trong đó, xác định rõ mức độ ảnh hưởng đến hệ thống thông tin đang được đề xuất cấp độ khi các hệ thống này bị mất an toàn thông tin;

2) Danh mục đề xuất các thành phần, thiết bị mạng quan trọng và mức độ quan trọng;

3) Thuyết minh về các nguy cơ tấn công mạng, mất an toàn thông tin đối với hệ thống và các ảnh hưởng;

4) 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;

5) Thuyết minh yêu cầu cần phải vận hành 24/7 và không chấp nhận ngừng vận hành mà không có kế hoạch trước.

Ví dụ: Đối với Hệ thống thông tin B được đề xuất là cấp độ 4 như sau:

1) Danh mục các hệ thống thông tin khác có kết nối hoặc có liên quan và đến hệ thống thông tin B và mức độ ảnh hưởng đến hệ thống thông tin B khi các hệ thống này bị mất an toàn thông tin:

- Hệ thống mạng của ISP, hệ thống này khi có sự cố sẽ làm mất kết nối và truy cập từ xa từ các hệ thống thành phần về hệ thống trung tâm qua kết nối VPN.

- Hệ thống cơ sở dữ liệu quốc gia về điện lực, hệ thống này khi bị mất an toàn thông tin sẽ làm lộ lọt thông tin liên quan đến hoạt động kinh doanh, sản xuất, sự an toàn công trình của Nhà máy Thủy điện/Công trình thủy lợi B (hệ thống khi bị phá hoại sẽ làm tổn hại nghiêm trọng).

2) Danh mục đề xuất các thành phần, thiết bị mạng và mức độ quan trọng:

STT	Tên thiết bị	Thông tin xử lý	Chức năng/ Mức độ quan trọng
1	Router01	Toàn bộ thông tin từ bên trong mạng trao đổi với các mạng bên ngoài hệ thống trung tâm	Kết nối hệ thống với các mạng bên ngoài; làm mất toàn bộ kết nối tới các mạng bên ngoài hệ thống khi gặp sự cố
2	Firewall01	Thông tin vào/ra vùng mạng OT từ mạng IT	Quản lý truy cập và bảo vệ vùng mạng OT; làm mất ATTT cho hệ thống máy chủ điều khiển khi bị chiếm quyền điều khiển hoặc xảy ra sự cố
3	SCADA-Server01	Thông tin điều khiển hoạt động của hệ thống và dữ liệu giám sát	Lưu trữ và quản lý thông tin điều khiển hoạt động của hệ thống và dữ liệu giám sát; làm ngừng hoạt động hoặc làm phá hoại dữ liệu hệ thống khi bị chiếm quyền điều khiển hoặc xảy ra sự cố
4	...		

3) Thuyết minh về các nguy cơ tấn công mạng, mất an toàn thông tin đối với hệ thống và các ảnh hưởng:

- Nguy cơ tấn công, chiếm quyền điều khiển thông qua các điểm yếu an toàn thông tin và các máy chủ điều khiển làm ngừng hoạt động của toàn bộ hệ thống;

- Nguy cơ tấn công mạng mã độc vào các máy tính của cán bộ quản trị hệ thống, làm lộ lọt thông tin quản trị hệ thống, dẫn tới các máy chủ hệ thống bị chiếm quyền điều khiển hoặc bị phá hủy;

- Nguy cơ tấn công từ mạng IT (Information Technology) sang mạng OT (Operator Technology);

- Mô tả các nguy cơ tấn công khác (nếu có).

4) 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.

Ví dụ: Hệ thống được sử dụng để điều khiển hoạt động bình thường của Công trình Thủy điện/thủy điện B trên địa bàn tỉnh Q, khi bị phá hoại sẽ làm ngừng cung cấp điện cho toàn bộ nhà máy, các hộ dân trên địa bàn tỉnh, làm ảnh hưởng đặc biệt nghiêm trọng tới lợi ích công cộng.

5) Thuyết minh yêu cầu cần phải vận hành 24/7 và không chấp nhận ngừng vận hành mà không có kế hoạch trước.

Ví dụ: Do đặc thù của hệ thống là cung cấp điện phục vụ sản xuất, kinh doanh của các nhà máy, doanh nghiệp trên địa bàn, do đó yêu cầu hệ thống phải đảm bảo hoạt động 24/7.

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

Hướng dẫn chung: *Đối với các hệ thống thông tin/hệ thống thành phần độc lập về hạ tầng, đơn vị vận hành và chính sách quản lý thì xây dựng phương án bảo đảm an toàn thông tin riêng cho từng hệ thống đó.*

Phương án bảo đảm an toàn thông tin đối với hệ thống thông tin mới, cần chỉ ra phương án triển khai cụ thể khi xây dựng và thiết lập hệ thống. ***Ví dụ*** *để đáp ứng yêu cầu an toàn thông tin nào thì sử dụng giải pháp gì, phương án triển khai thế nào.*

Phương án bảo đảm an toàn thông tin đối với hệ thống đã đưa vào quản lý vận hành, cần chỉ rõ các yêu cầu nào đã đáp ứng và mô tả ngắn gọn giải pháp và phương án đã triển khai. Đối với các yêu cầu chưa đáp ứng, cần mô tả phương án dự kiến sẽ sử dụng là gì, kế hoạch và lộ trình triển khai để đáp ứng yêu cầu an toàn.

Để thuyết minh chi tiết việc đáp ứng các yêu cầu an toàn quy định tại Thông tư 03, có thể tham khảo các yêu cầu an toàn cụ thể tại Tiêu chuẩn quốc gia TCVN 11930:2017 về yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ.

1. Yêu cầu quản lý

Hướng dẫn: *Tùy theo cấp độ đề xuất tương ứng, thuyết minh phương án bảo đảm an toàn thông tin đáp ứng ứng các yêu cầu quản lý cần:*

- Đối với hệ thống thông tin xây dựng mới phải có dự thảo Chính sách an toàn thông tin đáp ứng các yêu cầu quản lý được quy định trong Thông tư 03 và được thuyết minh theo hướng dẫn trong tài liệu này, được Chủ quản hệ thống thông tin ban hành sau khi đưa hệ thống vào vận hành, khai thác.

- Đối với hệ thống thông tin đã đưa vào vận hành, khai thác phải có Chính sách an toàn thông tin hoặc Quy chế bảo đảm an toàn thông tin đáp ứng các yêu cầu quản lý được quy định trong Thông tư 03 và được thuyết minh theo hướng dẫn trong tài liệu này, được Chủ quản hệ thống thông tin phê duyệt ban hành.

Thuyết minh phương án đáp ứng yêu cầu quản lý theo cấu trúc sau:

1.1. Mục tiêu, nguyên tắc bảo đảm an toàn thông tin

1.2. Trách nhiệm của đơn vị chuyên trách về an toàn thông tin, các cán bộ làm về an toàn thông tin, người sử dụng đầu cuối, các đối tượng thuộc phạm vi điều chỉnh của chính sách an toàn thông tin

1.3. Phạm vi chính sách an toàn thông tin

1.4. **Tổ chức** bảo đảm an toàn thông tin

1.5. Bảo đảm nguồn **nhân lực**

1.6. Quản lý thiết kế, xây dựng hệ thống *(cấp độ 2 trở lên)*

1.7. Quản lý vận hành hệ thống

- Quản lý an toàn máy chủ
- Quản lý an toàn ứng dụng
- Quản lý an toàn dữ liệu
- Quản lý an toàn mạng *(cấp độ 2 trở lên)*
- Quản lý sự cố an toàn thông tin
- Quản lý an toàn người sử dụng đầu cuối

Đối với hệ thống thông tin cấp độ 3 trở lên cần bổ sung:

- 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
- Quản lý điểm yếu an toàn thông tin.

1.8. Kiểm tra, đánh giá và quản lý rủi ro *(cấp độ 2 trở lên)*

2. Yêu cầu kỹ thuật

Hướng dẫn: *Tùy thuộc vào đặc trưng của từng hệ thống cụ thể, việc thuyết minh phương án bảo đảm an toàn thông tin có thể thuyết minh cho phù hợp với đặc thù của hệ thống đó.*

Ví dụ: Trường hợp có hệ thống thông tin có tính chất đặc thù như hệ thống điều khiển công nghiệp, không có kết nối Internet, thì không phải thuyết minh phương án phòng chống DDoS hay thiết kế vùng mạng DMZ…

Chú ý: Một yêu cầu kỹ thuật có thể thực hiện bằng nhiều phương án khác nhau. Đối với các hệ thống thông tin cấp độ 1,2 hoặc cấp độ 3 để giảm thiểu chi phí đầu tư thì để đáp ứng các yêu cầu kỹ thuật không nhất thiết phải đầu tư các thiết bị chuyên dụng mà có thể sử dụng chia sẻ hoặc đưa ra phương án tương đương khác.

Ví dụ: Yêu cầu về phương án xử lý tấn công DDoS thì có thể thuê dịch vụ hoặc xây dựng phương án xử lý riêng của mình, dựa trên năng lực hệ thống hiện có, thay vì đầu tư thiết bị xử lý tấn công DDoS chuyên dụng.

Thuyết minh phương án đáp ứng yêu cầu kỹ thuật theo cấu trúc sau:

2.1. Bảo đảm an toàn mạng *(cấp độ 2 trở lên)*

a) Thiết kế hệ thống

b) Kiểm soát truy cập từ bên ngoài mạng

c) Kiểm soát truy cập từ bên trong mạng

d) Nhật ký hệ thống

e) Phòng chống xâm nhập

f) Phòng chống phần mềm độc hại trên môi trường mạng

g) Bảo vệ thiết bị hệ thống

2.2. Bảo đảm an toàn máy chủ

a) Xác thực

b) Kiểm soát truy cập

c) Nhật ký hệ thống

d) Phòng chống xâm nhập

e) Phòng chống phần mềm độc hại

f) Xử lý máy chủ khi chuyển giao

2.3. Bảo đảm an toàn ứng dụng

a) Xác thực

b) Kiểm soát truy cập

c) Nhật ký hệ thống

d) Bảo mật thông tin liên lạc

e) Chống chối bỏ

2.4. Bảo đảm an toàn dữ liệu

a) Nguyên vẹn dữ liệu

b) Bảo mật dữ liệu

c) Sao lưu dự phòng

Lưu ý: Nghiên cứu hướng dẫn tại Điều 8, Điều 9 và các Phụ lục từ 1 đến 5 của Thông tư số 12/2022/TT-BTTTT ngày 12/ 8/ 2022 của Bộ trưởng Bộ Thông tin và Truyền thông.

PHẦN C: MẪU VĂN BẢN XÁC ĐỊNH CẤP ĐỘ AN TOÀN HỆ THỐNG THÔNG TIN

Mẫu số 01: Văn bản đề nghị thẩm định và phê duyệt hồ sơ đề xuất cấp độ 1, 2

(TÊN CƠ QUAN, TỔ CHỨC) **-------**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc** **----------**
Số: …….. V/v đề nghị thẩm định và phê duyệt hồ sơ đề xuất cấp độ an toàn HTTT	*....., 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 và phê duyệt hồ sơ đề xuất cấp độ an toàn hệ thống thông tin:

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 thuyết minh Hồ sơ đề xuất cấp độ (bao gồm: Thuyết minh tổng quan về hệ thống thông tin; Thuyết minh về việc đề xuất cấp độ căn cứ trên các tiêu chí theo quy định của pháp luật; Thuyết minh phương án bảo đảm an toàn thông tin theo cấp độ tương ứng).

2. Tài liệu thiết kế hệ thống.

Đề nghị (Đơn vị chuyên trách về an toàn thông tin) xem xét thẩm định và phê duyệt./.

Nơi nhận: - Như trên; - ……..	**ĐẠI DIỆN CỦA CƠ QUAN, TỔ CHỨC** *(Ký, ghi rõ họ tên, chức danh và đóng dấu)*

Mẫu số 02: Văn bản đề nghị thẩm định hồ sơ đề xuất cấp độ 3

(TÊN CƠ QUAN, TỔ CHỨC) **-------**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc** **----------**
Số: …….. V/v đề nghị thẩm định hồ sơ đề xuất cấp độ an toàn HTTT	*....., ngày ... tháng ... năm ...*

Kính gửi: (Đơn vị chuyên trách về an toàn thông tin/đơn vị thẩm định).

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 thẩm định) thẩm định hồ sơ đề xuất cấp độ an toàn hệ thống thông tin:

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 thuyết minh Hồ sơ đề xuất cấp độ (bao gồm: Thuyết minh tổng quan về hệ thống thông tin; Thuyết minh về việc đề xuất cấp độ căn cứ trên các tiêu chí theo quy định của pháp luật; Thuyết minh phương án bảo đảm an toàn thông tin theo cấp độ tương ứng).

2. Tài liệu thiết kế hệ thống.

Đề nghị (đơn vị thẩm định) xem xét, thẩm định./.

Nơi nhận: - Như trên; - ……..	**ĐẠI DIỆN CỦA CƠ QUAN, TỔ CHỨC** *(Ký, ghi rõ họ tên, chức danh và đóng dấu)*

Mẫu số 03: Văn bản xin ý kiến chuyên môn về hồ sơ đề xuất cấp độ 4, 5

(TÊN CƠ QUAN, TỔ CHỨC) **-------**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc** **----------**
Số: …….. V/v xin ý kiến chuyên môn về hồ sơ đề xuất cấp độ an toàn HTTT	*....., 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 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:

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 thuyết minh Hồ sơ đề xuất cấp độ (bao gồm: Thuyết minh tổng quan về hệ thống thông tin; Thuyết minh về việc đề xuất cấp độ căn cứ trên các tiêu chí theo quy định của pháp luật; Thuyết minh phương án bảo đảm an toàn thông tin theo cấp độ tương ứng).

2. Tài liệu thiết kế hệ thống.

Đề nghị (Đơn vị chuyên trách về an toàn thông tin) xem xét, cho ý kiến./.

Nơi nhận: - Như trên; - ……..	**ĐẠI DIỆN CỦA CƠ QUAN, TỔ CHỨC** *(Ký, ghi rõ họ tên, chức danh và đóng dấu)*

Mẫu số 04: Văn bản đề nghị thẩm định hồ sơ đề xuất cấp độ 4, 5

(TÊN CƠ QUAN, TỔ CHỨC) **-------**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc** **----------**
Số: …….. V/v đề nghị thẩm định hồ sơ đề xuất cấp độ an toàn HTTT	*....., ngày ... tháng ... năm ...*

Kính gửi: (Bộ TTTT/Bộ Quốc phòng/Bộ Công an).

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 (Bộ TT&TT/Bộ Quốc phòng/Bộ Công an) thẩm định hồ sơ đề xuất cấp độ an toàn hệ thống thông tin:

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 thuyết minh Hồ sơ đề xuất cấp độ (bao gồm: Thuyết minh tổng quan về hệ thống thông tin; Thuyết minh về việc đề xuất cấp độ căn cứ trên các tiêu chí theo quy định của pháp luật; Thuyết minh phương án bảo đảm an toàn thông tin theo cấp độ tương ứng).

2. Tài liệu thiết kế hệ thống.

3. Ý kiến về mặt chuyên môn của đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin.

Kính đề nghị (Bộ TTTT/Bộ Quốc phòng/Bộ Công an) xem xét, thẩm định./.

Nơi nhận: - Như trên; - ……..	**ĐẠI DIỆN CỦA CƠ QUAN, TỔ CHỨC** *(Ký, ghi rõ họ tên, chức danh và đóng dấu)*

Mẫu số 05: Văn bản đề nghị phê duyệt hồ sơ đề xuất cấp độ 3, 4

(TÊN CƠ QUAN, TỔ CHỨC)	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**
-------	**Độc lập - Tự do - Hạnh phúc**

Số: …….	*....., ngày ... tháng ... năm ...*
V/v đề nghị phê duyệt hồ sơ đề xuất cấp độ an toàn HTTT	

Kính gửi: (Cơ quan chủ quản 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),

(Tên cơ quan, tổ chức) đề nghị (Cơ quan chủ quản hệ thống thông tin) phê duyệt hồ sơ đề xuất cấp độ an toàn hệ thống thông tin:

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 phê duyệt:

Phần 2. Hồ sơ kèm theo

1. Tài liệu thuyết minh Hồ sơ đề xuất cấp độ (bao gồm: Thuyết minh tổng quan về hệ thống thông tin; Thuyết minh về việc đề xuất cấp độ căn cứ trên các tiêu chí theo quy định của pháp luật; Thuyết minh phương án bảo đảm an toàn thông tin theo cấp độ tương ứng).

2. Tài liệu thiết kế hệ thống.

3. Kết quả thẩm định Hồ sơ đề xuất cấp độ.

Kính đề nghị (Cơ quan chủ quản hệ thống thông tin) xem xét, phê duyệt./.

Nơi nhận:	**ĐẠI DIỆN CỦA CƠ QUAN, TỔ CHỨC**
- Như trên;	*(Ký, ghi rõ họ tên, chức danh và đóng dấu)*
- ……..	

Mẫu số 06: Văn bản đề nghị phê duyệt phương án bảo đảm an toàn thông tin đối với hệ thống thông tin cấp độ 5

(TÊN CƠ QUAN, TỔ CHỨC) **-------**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc** **----------**
Số: …….. V/v đề nghị phê duyệt phương án bảo đảm an toàn HTTT cấp độ 5	*....., ngày ... tháng ... năm ...*

Kính gửi: (Cơ quan chủ quản 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),

(Tên cơ quan, tổ chức) đề nghị (Cơ quan chủ quản hệ thống thông tin) phê duyệt phương án bảo đảm an toàn thông tin đối với hệ thống thông tin cấp độ 5:

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 HTTT đề xuất phê duyệt phương án bảo đảm: 5

Phần 2. Hồ sơ kèm theo

1. Tài liệu thuyết minh Hồ sơ đề xuất cấp độ (bao gồm: Thuyết minh tổng quan về hệ thống thông tin; Thuyết minh về việc đề xuất cấp độ căn cứ trên các tiêu chí theo quy định của pháp luật; Thuyết minh phương án bảo đảm an toàn thông tin theo cấp độ tương ứng).

2. Tài liệu thiết kế hệ thống.

3. Kết quả thẩm định Hồ sơ đề xuất cấp độ của (Bộ TTTT/Bộ Quốc phòng/Bộ Công an).

Kính đề nghị (Cơ quan chủ quản hệ thống thông tin) xem xét, phê duyệt phương án bảo đảm an toàn thông tin./.

Nơi nhận: - Như trên; - ……..	**ĐẠI DIỆN CỦA CƠ QUAN, TỔ CHỨC** *(Ký, ghi rõ họ tên, chức danh và đóng dấu)*

Mẫu số 07: Quyết định phê duyệt cấp độ an toàn hệ thống thông tin

(CHỦ QUẢN HỆ THỐNG THÔNG TIN)	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**
	Độc lập - Tự do - Hạnh phúc
-------	----------
Số: ……..	*....., ngày ... tháng ... năm ...*

QUYẾT ĐỊNH

Về việc phê duyệt cấp độ an toàn hệ thống thông tin

(THỦ TRƯỞNG CƠ QUAN TỔ CHỨC)

Căn cứ Luật an toàn thông tin mạng ngày 19 tháng 11 năm 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),

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 này.

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;

ĐẠI DIỆN CỦA CƠ QUAN, TỔ CHỨC
(Ký, ghi rõ họ tên, chức danh và đóng dấu)

Mẫu số 08: Quyết định phê duyệt phương án bảo đảm an toàn thông tin

(CHỦ QUẢN HỆ THỐNG THÔNG TIN)	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**
-------	**Độc lập - Tự do - Hạnh phúc**
Số: ……..	**----------**
	....., ngày ... tháng ... năm ...

QUYẾT ĐỊNH

Về việc phê duyệt phương án bảo đảm an toàn thông tin

(THỦ TRƯỞNG CƠ QUAN TỔ CHỨC)

Căn cứ Luật an toàn thông tin mạng ngày 19 tháng 11 năm 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),

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 này.

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;
- ……..

ĐẠI DIỆN CỦA CƠ QUAN, TỔ CHỨC
(Ký, ghi rõ họ tên, chức danh và đóng dấu)