

UBND TỈNH GIA LAI
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 1202/STTTT-CNTT
V/v hướng dẫn thực hiện công tác
xác định cấp độ an toàn thông tin

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

Gia Lai, ngày 19 tháng 11 năm 2018

Kính gửi:

- Văn phòng Tỉnh ủy;
- Văn phòng Đoàn Đại biểu Quốc hội tỉnh;
- Văn phòng Hội đồng nhân dân tỉnh;
- Văn phòng Ủy ban nhân dân tỉnh;
- Văn phòng Ủy ban MTTQ Việt Nam tỉnh;
- Bộ Chỉ huy Quân sự tỉnh Gia Lai;
- Công an tỉnh Gia Lai;
- Các Sở, ban, ngành thuộc tỉnh;
- Các Hội, Đoàn thể của tỉnh;
- Ủy ban nhân dân các huyện, thị xã, thành phố.

Thực hiện chỉ đạo của UBND tỉnh theo nội dung Công văn số 2035/VP-KGVX ngày 19/7/2018 về việc đôn đốc, hướng dẫn thực hiện công tác xác định cấp độ và xây dựng Hồ sơ đề xuất cấp độ an toàn hệ thống thông tin, nhằm thực hiện nhiệm vụ được giao và tăng cường công tác đảm bảo an toàn thông tin mạng của các cơ quan, đơn vị trên địa bàn tỉnh, Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị triển khai thực hiện các nội dung sau:

1. Xác định cấp độ an toàn hệ thống thông tin của các hệ thống thông tin thuộc phạm vi đơn vị quản lý.

2. Xây dựng Hồ sơ đề xuất cấp độ, sau đó gửi Sở Thông tin và Truyền thông thẩm định và phê duyệt (đối với Hồ sơ đề xuất cấp độ 1, 2) hoặc thẩm định, trình cơ quan có thẩm quyền phê duyệt theo quy định (đối với Hồ sơ đề xuất cấp độ 3, 4 hoặc 5). Trong đó, phương án bảo đảm an toàn thông tin trong Hồ sơ đề xuất phải đáp ứng các yêu cầu an toàn theo tiêu chuẩn quốc gia TCVN 11930:2017 về yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ, trình cấp có thẩm quyền phê duyệt theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

3. 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.

4. Thời hạn gửi hồ sơ và kết quả về Sở Thông tin và Truyền thông: **trước ngày 06/12/2018.**

Sở Thông tin và Truyền thông gửi kèm theo một số tài liệu hướng dẫn xác định cấp độ và xây dựng Hồ sơ đề xuất cấp độ an toàn thông tin:

- Phụ lục I: Một số nội dung hướng dẫn triển khai thực hiện.

- Phụ lục II: Hướng dẫn lập hồ sơ đề xuất cấp độ an toàn thông tin và hồ sơ tham khảo.

Tài liệu được đăng tải trên Trang thông tin điện tử tại địa chỉ: <http://stttt.gialai.gov.vn>, mục Văn bản/Văn bản Sở TTTT/Công nghệ thông tin và điện tử.

Trong quá trình thực hiện, nếu có vướng mắc đề nghị các cơ quan, đơn vị liên hệ Phòng Công nghệ thông tin – Sở Thông tin và Truyền thông để phối hợp thực hiện (ĐT: 02693.719.653, Email: quyenntn.stttt@gialai.gov.vn, gặp Đ/c Nguyễn Thị Ngọc Quyên).

Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị quan tâm, triển khai thực hiện./.

Nơi nhận:

- Như trên;
- UBND tỉnh (Báo cáo);
- Trung tâm CNTT&TT;
- Lưu: VT, P.CNTT.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Dặng Quang Khanh



PHỤ LỤC I:

MỘT SỐ NỘI DUNG HƯỚNG DẪN TRIỂN KHAI THỰC HIỆN

*(Kèm theo Công văn số 1202/STTTT-CNTT ngày 19/11/2018
của Sở Thông tin và Truyền thông)*

1. Các thuật ngữ về *Chủ quản hệ thống thông tin, Đơn vị vận hành hệ thống thông tin, Đơn vị chuyên trách về công nghệ thông tin, Đơn vị chuyên trách về an toàn thông tin, Bộ phận chuyên trách về an toàn thông tin* được định nghĩa, giải thích tại Điều 3 Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn thông tin theo cấp độ (gọi tắt là Nghị định số 85/2016/NĐ-CP) và Điều 5, Điều 6 Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ (gọi tắt là Thông tư số 03/2017/TT-BTTTT).

2. Việc phân loại thông tin và hệ thống thông tin được quy định tại Điều 6 Nghị định số 85/2016/NĐ-CP và hướng dẫn tại Điều 4 Thông tư số 03/2017/TT-BTTTT; nguyên tắc xác định cấp độ, việc xác định cấp độ và thuyết minh cấp độ an toàn hệ thống thông tin thực hiện theo quy định tại Điều 5, Điều 7, Điều 8, Điều 9, Điều 10, Điều 11 Nghị định số 85/2016/NĐ-CP và hướng dẫn tại Điều 7 Thông tư số 03/2017/TT-BTTTT; việc xây dựng phương án bảo đảm an toàn thông tin theo cấp độ tương ứng phải đáp ứng các yêu cầu, nội dung quy định tại Điều 19 Nghị định số 85/2016/NĐ-CP và hướng dẫn tại Điều 8, Điều 9 Thông tư số 03/2017/TT-BTTTT.

3. Thẩm quyền thẩm định và phê duyệt cấp độ; hồ sơ đề xuất cấp độ, hồ sơ phê duyệt đề xuất cấp độ; trình tự thủ tục xác định, xác định lại cấp độ, thẩm định, phê duyệt hồ sơ đề xuất cấp độ an toàn hệ thống thông tin được quy định từ Điều 12 đến Điều 18 Nghị định số 85/2016/NĐ-CP và hướng dẫn từ Điều 14 đến Điều 16 Thông tư số 03/2017/TT-BTTTT.

4. Đối với hệ thống thông tin được đề xuất cấp độ 1, 2, 3 của các cơ quan, đơn vị, đề nghị lập theo mẫu (*gửi kèm theo*) gửi về Sở Thông tin và Truyền thông 01 bản chính và 02 bản sao hồ sơ hợp lệ để thẩm định.

5. Đối với hệ thống thông tin được đề xuất cấp độ 4, 5, đơn vị vận hành hệ thống thông tin gửi 01 bộ hồ sơ hợp lệ về Sở Thông tin và Truyền thông để xem xét, có ý kiến, trình cấp có thẩm quyền thẩm định, phê duyệt.

PHỤ LỤC II: HƯỚNG DẪN LẬP HỒ SƠ ĐỀ XUẤT CẤP ĐỘ AN TOÀN HỆ THỐNG THÔNG TIN VÀ HỒ SƠ THAM KHẢO

(Kèm theo Công văn số /STTTT-CNTT ngày /11/2018
của Sở Thông tin và Truyền thông)

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

Hồ sơ đề xuất cấp độ cơ bản gồm 02 loại tài liệu bản cứng: *Tài liệu thuyết minh Hồ sơ đề xuất cấp độ và Tài liệu thiết kế hệ thống*. Ngoài ra, có thêm văn bản ý kiến về mặt chuyên môn của đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin (Sở Thông tin và Truyền thông) đối với hệ thống thông tin đề xuất cấp độ 4 hoặc cấp độ 5.

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.

Hồ sơ đề xuất cấp độ theo hướng dẫn sau:

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

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

Gia Lai - 2018

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 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 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 dân 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/Trang thông tin điện tử.
- + Hệ thống thư điện tử công vụ.

- + Hệ thống Quản lý tài sản công.
- + Hệ thống quản lý CBCCVC.
- + 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 đặc thù theo chức năng và không có những vùng mạng được đưa ra như trong Thông tư số 03/2017/TT-BTTTT của Bộ TT&TT 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 03) thì việc mô tả cấu trúc của hệ thống thông tin đó được mô tả theo cấu trúc thực tế của hệ thống.

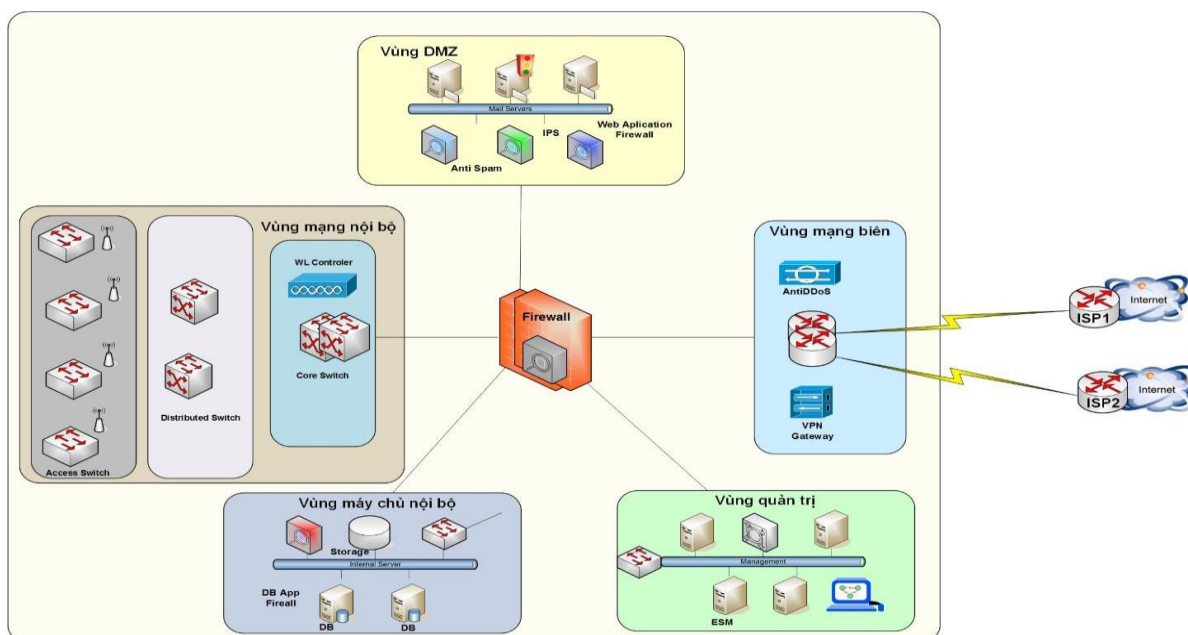
b) *Cấu trúc vật lý mô tả các thiết bị mạng, các thiết bị đầu cuối có trong hệ thống và các kết nối vật lý giữa các thiết bị.*

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 và điều hành, một cửa điện tử, ... và các dịch vụ hệ thống như DNS, DHCP, FTP...): 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

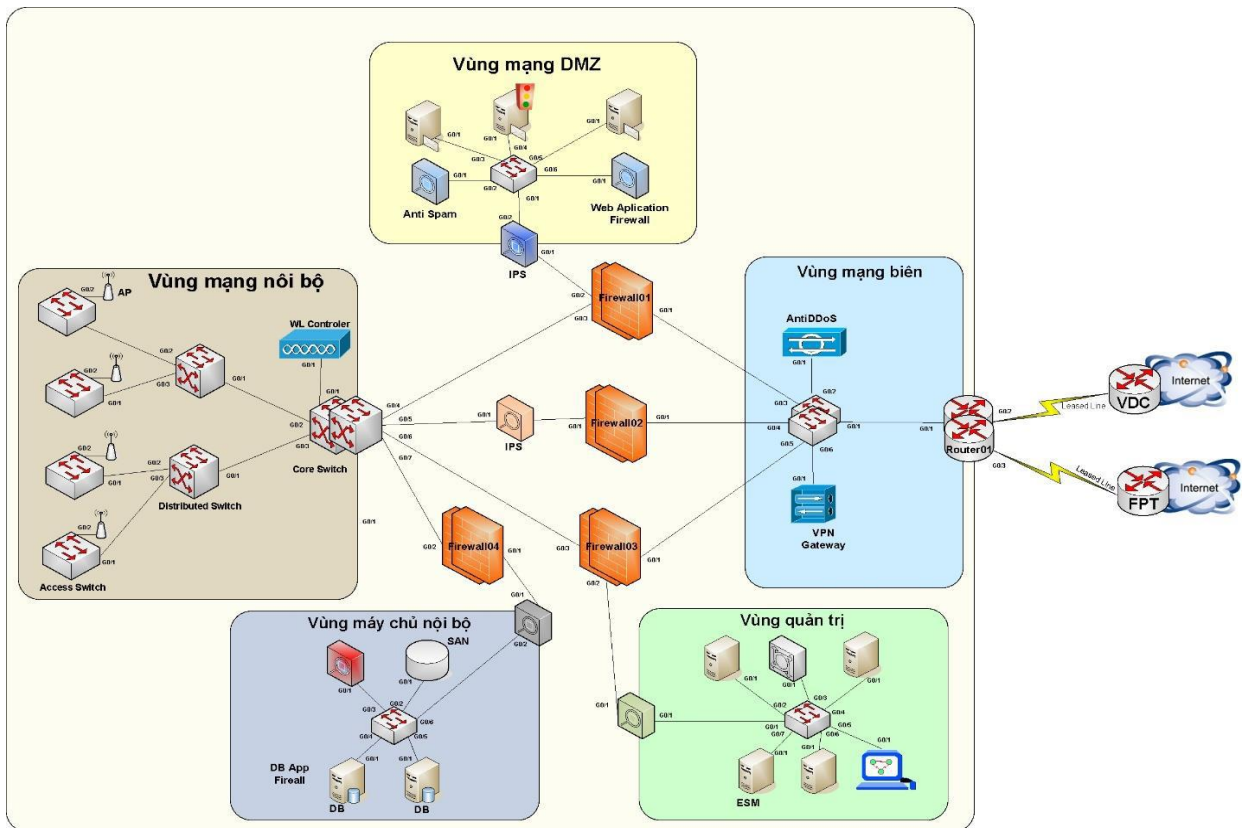


Hình 1: Cấu trúc logic của hệ thống A

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/SOPHOS	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, giải

	tử	bộ/ Centos7	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 khách 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 cơ quan, đơn vị		Hệ thống cơ sở hạ tầng thông tin dùng chung phục vụ hoạt động của một cơ quan, tổ chức.	2	Khoản 3, Điều 8 Nghị định số 85/2016/NĐ-CP
2	Phòng máy chủ/Trung tâm tích hợp dữ liệu của cơ quan, đơn vị		Hệ thống cơ sở hạ tầng thông tin dùng chung phục vụ hoạt động của một cơ quan, tổ chức.	3	Khoản 3, Điều 9 Nghị định số 85/2016/NĐ-CP
3	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
4	Hệ thống một cửa điện tử 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
5	Cổng/Trang thông tin điện tử của cơ quan, đơn vị	Thông tin công cộng	Hệ thống thông tin phục vụ người dân, doanh nghiệp,	2	Điểm a, Khoản 2, Điều 8 Nghị định số 85/2016/NĐ-CP

			cung cấp thông tin và DVC trực tuyến từ mức độ 2 trở xuống		
6	Hệ thống quản lý CBCCVC	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
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	Hệ thống Dịch vụ công trực tuyến	Thông tin công cộng	Hệ thống thông tin phục vụ người dân, doanh nghiệp	3	Điểm a, Khoản 2, Điều 9 Nghị định số 85/2016/NĐ-CP
...					

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 03. 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 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 03/2017/TT-BTTTT.

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: Sở Thông tin và Truyền thông.

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 Sở Thông tin và Truyền thông 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:

....., ngày ... tháng ... năm ...

V/v đề nghị thẩm định hồ sơ
đề xuất cấp độ an toàn HTTT

Kính gửi: Sở Thông tin và Truyền thông.

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 Sở Thông tin và Truyền thông 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 Sở Thông tin và Truyền thông 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:

....., ngày ... tháng ... năm ...

V/v xin ý kiến chuyên môn về hồ sơ
đề xuất cấp độ an toàn HTTT

Kính gửi: Sở Thông tin và Truyền thông.

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 Sở Thông tin và Truyền thông 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 Sở Thông tin và Truyền thông 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:

....., ngày ... tháng ... năm ...

V/v đề nghị thẩm định hồ sơ
đề xuất cấp độ an toàn HTTT

Kính gửi: (Bộ TT&TT/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 TT&TT/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:

- Như trên;

-

ĐẠI DIỆN CỦA CƠ QUAN, TỔ CHỨC

(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:

....., ngày ... tháng ... năm ...

V/v đề nghị phê duyệt phương án
bảo đảm an toàn HTTT cấp độ 5

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 TT&TT/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)