BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

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

Số: 713 /CATTT-TĐQLGS
V/v hướng dẫn xác định và thực thi bảo vệ hệ thống thông tin theo cấp độ

Hà Nội, ngày 25 tháng 7 năm 2019

Kính gửi:

- Đơn vị chuyên trách về CNTT của các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương;
- Tập đoàn kinh tế, Tổng công ty Nhà nước.

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

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

Căn cứ Thông tư số 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP/2016/NĐ-CP ngày 01 tháng 7 năm 2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Cục An toàn thông tin công bố Tài liệu "Hướng dẫn xác định và thực thi bảo vệ hệ thống thông tin theo cấp độ". Tài liệu hướng dẫn này đưa ra các quy định của nhà nước về bảo đảm an toàn hệ thống thông tin theo cấp độ là cơ sở để cơ quan, tổ chức có thể xác định được những hệ thống thông tin cần bảo vệ, thuộc phạm vi quản lý của mình và triển khai các phương án bảo vệ hiệu quả, giảm thiểu chi phí đầu tư.

Bản mềm tài liệu hướng dẫn có thể được tải về từ cổng thông tin điện tử của Cục An toàn thông tin tại địa chỉ: https://www.ais.gov.vn/huong-dan-xac-dinh-va-thuc-thi-bao-ve-he-thong-thong-tin-theo-cap-do.htm.

Chi tiết liên hệ ông Nguyễn Tiến Đức, Phòng Thẩm định và Quản lý giám sát, Cục An toàn thông tin, Điện thoại: 0934578162; Thư điện tử: ntduc@mic.gov.vn;

Trong quá trình thực hiện, nếu có điều gì vướng mắc, đề nghị các cơ quan, tổ chức phản ánh về Cục An toàn thông tin để được hướng dẫn thực hiện./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Thành Hưng (để b/c);
- Lưu: VT, P.TĐQLGS.

CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC AN TOÀN THÔNG TIN
BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Huy Dũng

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

TÀI LIỆU HƯỚNG DẪN
XÁC ĐỊNH VÀ THỰC THI BẢO VỆ HỆ THỐNG THÔNG TIN THEO CẤP ĐỘ

(*Kèm theo Công văn số /CATTT-TĐQLGS*
ngày tháng năm 2019 của Cục An toàn thông tin)

Hà Nội, 2019

Chương I
PHẠM VI, ĐỐI TƯỢNG ÁP DỤNG

1.1. Phạm vi áp dụng

Tài liệu này hướng dẫn việc xác định và thực thi bảo đảm an toàn hệ thống thông tin theo cấp độ bao gồm các nội dung: Xác định các chủ thể liên quan; Hướng dẫn xác định cấp độ; Quy trình thẩm định và phê duyệt cấp độ; Hướng dẫn xây dựng Hồ sơ đề xuất cấp độ; Hướng dẫn thẩm định Hồ sơ đề xuất cấp độ; Hướng dẫn bảo vệ hệ thống thông tin theo cấp độ; Hồ sơ đề xuất cấp độ mẫu.

1.2. Đối tượng áp dụng

Tài liệu này áp dụng đối với cơ quan, tổ chức, cá nhân tham gia hoặc có liên quan đến hoạt động xây dựng, thiết lập, quản lý, vận hành, nâng cấp, mở rộng hệ thống thông tin tại Việt Nam phục vụ ứng dụng công nghệ thông tin trong hoạt động của cơ quan, tổ chức nhà nước, ứng dụng công nghệ thông tin trong việc cung cấp dịch vụ trực tuyến phục vụ người dân và doanh nghiệp.

Khuyến khích tổ chức, cá nhân liên quan khác tham khảo tài liệu này để có biện pháp bảo vệ hệ thống thông tin phù hợp.

Chương II
HƯỚNG DẪN XÁC ĐỊNH CHỦ THỂ LIÊN QUAN

Chủ thể liên quan trong tài liệu này bao gồm: Chủ quản hệ thống thông tin, Đơn vị chuyên trách an toàn thông tin, Đơn vị vận hành hệ thống thông tin. Việc xác định chủ thể liên quan phụ thuộc vào cơ cấu, tổ chức của mỗi cấp và được hướng dẫn chi tiết ở dưới đây:

2.1. Chủ quản hệ thống thông tin

Chủ quản hệ thống thông tin được xác định căn cứ quy định tại Điều 5 Thông tư 03/2017/TT-BTTTT, bao gồm các trường hợp sau:

1) Chủ quản của hệ thống thông tin thuộc phạm vi quản lý của cơ quan, tổ chức nhà nước được xác định trong các trường hợp sau:

a) Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ được xác định tại Quyết định số 02/2002/QH11 ngày 05/08/2012 quy định danh sách các Bộ và cơ quan ngang Bộ của Chính phủ.

b) Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương là một cơ quan hành chính nhà nước của hệ thống hành chính nhà nước, là cơ quan thực thi pháp luật tại các cấp tỉnh, thành phố trực thuộc Trung ương.

c) Trường hợp Chủ quản hệ thống thông tin không phải là hai trường hợp ở trên thì Chủ quản được xác định là cấp có thẩm quyền quyết định đầu tư dự án xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin.

2) Hệ thống thông tin thuộc phạm vi quản lý của doanh nghiệp và tổ chức khác.

Trong trường hợp này, Chủ quản hệ thống thông tin là cấp có thẩm quyền quyết định đầu tư dự án xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin.

Ví dụ: Là tổ chức đại diện theo pháp luật của công ty mẹ thuộc Tập đoàn kinh tế và tổng công ty, được tổ chức dưới hình thức công ty trách nhiệm hữu hạn một thành viên do Nhà nước làm chủ sở hữu hoặc trường hợp công ty mẹ là công ty cổ phần, công ty trách nhiệm hữu hạn hai thành viên trở lên có cổ phần, vốn góp chi phối của Nhà nước.

Lưu ý: Trường hợp, để thuận tiện cho quá trình đầu tư xây dựng và quản lý vận hành hệ thống, Chủ quản hệ thống thông tin có thể ủy quyền cho một tổ chức thay mặt mình thực hiện quyền quản lý trực tiếp đối với hệ thống thông tin. Việc uỷ quyền phải được thực hiện bằng văn bản, trong đó nêu rõ phạm vi và thời hạn uỷ quyền. Tổ chức được ủy quyền phải trực tiếp thực hiện quyền và nghĩa vụ của chủ quản hệ thống thông tin mà không được ủy quyền lại cho bên thứ ba theo quy định tại khoản 3, Điều 5 Thông tư 03/2017/TT-BTTTT.

Ví dụ: Trường hợp Sở TT&TT của một tỉnh là đơn vị vận hành Trung tâm tích hợp dữ liệu của tỉnh đó thì để thuận tiện cho công tác thẩm định và phê duyệt Hồ sơ đề xuất cấp độ cho Trung tâm tích hợp dữ liệu, Ủy ban nhân dân tỉnh đó có thể ủy quyền cho Sở TT&TT tổ chức thay mặt thực hiện quyền quản lý trực tiếp Trung tâm dữ liệu. Trong trường hợp này, Sở TT&TT phải chỉ định và giao trách nhiệm cho đơn vị chuyên trách về an toàn thông tin (ví dụ Phòng CNTT) và đơn vị vận hành (ví dụ Trung tâm CNTT).

2.2. Đơn vị chuyên trách an toàn thông tin

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

Đối với các tổ chức chưa có đơn vị chuyên trách về an toàn thông tin độc lập, thì đơn vị chuyên trách về an toàn thông tin là đơn vị chuyên trách về công nghệ thông tin. Trong trường hợp này, chủ quản hệ thống thông tin có trách nhiệm (điểm b, khoản 1, Điều 20 Nghị định 85/2016/NĐ-CP/2016/NĐ-CP): (1) Chỉ định đơn vị chuyên trách về công nghệ thông tin làm nhiệm vụ đơn vị chuyên trách về an toàn thông tin; (2) Thành lập hoặc chỉ định bộ phận chuyên trách về an toàn thông tin trực thuộc đơn vị chuyên trách về công nghệ thông tin.

Ví dụ: Đơn vị chuyên trách về an toàn thông tin của các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ thường là Cục Công nghệ thông tin hoặc Trung tâm thông tin; Đơn vị chuyên trách về an toàn thông tin của Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương thường là các Sở TT&TT trên địa bàn; Đơn vị chuyên trách về an toàn thông tin của các doanh nghiệp thường là Ban CNTT, Trung tâm CNTT hoặc phòng CNTT.

2.3. Đơn vị vận hành

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

Đơn vị vận hành của Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ thường là Tổng Cục, Cục, Trung tâm, Viện... Các đơn vị này quản lý vận hành hệ thống thông tin phục vụ hoạt động chung của Bộ hoặc hệ thống thông tin phục vụ nhiệm vụ chuyên môn nghiệp vụ riêng của từng đơn vị.

Đơn vị vận hành của Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương thường là các Sở, ban, ngành, quận, huyện hoặc cơ quan khác trên địa bàn quản lý vận hành hệ thống thông tin phục vụ nhiệm vụ chuyên môn nghiệp vụ riêng của từng đơn vị.

Lưu ý: Đối với trường hợp Sở TT&TT là đơn vị quản lý vận hành Trung tâm tích hợp dữ liệu phục vụ hoạt động chung của cả tỉnh, thì Sở TT&TT vừa đóng vai trò là đơn vị vận hành đối với Trung tâm tích hợp dữ liệu. Nhưng đóng vai trò là đơn vị chuyên trách về an toàn thông tin đối với các Sở khác trên địa bàn.

Trong trường hợp này, Sở TT&TT có thể lựa chọn ba phương án:

- Phương án 1: Tham mưu UBND ủy quyền cho Sở TT&TT làm Chủ quản đối với Trung tâm tích hợp dữ liệu. Sở TT&TT chỉ định và giao trách nhiệm cho Phòng CNTT là đơn vị chuyên trách về an toàn thông tin và Trung tâm thông tin là đơn vị vận hành.

- Phương án 2: Đối với việc thẩm định và phê duyệt HSĐXCĐ đối với Trung tâm tích hợp dữ liệu, Sở TT&TT tham mưu UBND chỉ định một Sở trên địa bàn thẩm định (và phê duyệt với hệ thống cấp độ 1 hoặc cấp độ 2) HSĐXCĐ.

- Phương án 3: Trung tâm tích hợp dữ liệu là đơn vị vận hành, xây dựng HSĐXCĐ trình và gửi đơn vị chuyên trách về ATTT là Sở TT&TT cho ý kiến thẩm định, sau đó trình Chủ quản hệ thống thông tin thẩm định ở đây là UBND Tỉnh.

Đơn vị vận hành của doanh nghiệp và cơ quan, tổ chức khác là: Đơn vị thành viên của tổng công ty, Trung tâm kỹ thuật, đơn vị hoặc bộ phận được giao nhiệm vụ trực tiếp vận hành hệ thống thông tin.

Lưu ý:

- Trong trường hợp hệ thống thông tin bao gồm nhiều hệ thống thành phần hoặc phân tán, có nhiều hơn một đơn vị vận hành hệ thống thông tin, chủ quản hệ thống thông tin phải có trách nhiệm chỉ định một đơn vị làm đầu mối để thực hiện quyền và nghĩa vụ của đơn vị vận hành hệ thống thông tin theo quy định của pháp luật (khoản 2, Điều 6 Thông tư 03/2017/TT-BTTTT).

- Trong trường hợp chủ quản hệ thống thông tin thuê ngoài dịch vụ công nghệ thông tin, đơn vị vận hành hệ thống thông tin là bên cung cấp dịch vụ (khoản 3, Điều 6 Thông tư 03/2017/TT-BTTTT).

Chương III
HƯỚNG DẪN XÁC ĐỊNH CẤP ĐỘ

Cấp độ an toàn hệ thống thông tin được xác định căn cứ vào thông tin mà hệ thống đó xử lý và loại hình của hệ thống thông tin đó. Trên cơ sở đó, tiêu chí xác định cấp độ sẽ là tập các điều kiện giữa loại thông tin hệ thống đó xử lý và loại hình hệ thống thông tin. Việc xác định thông tin mà hệ thống xử lý và loại hình hệ thống thông tin được thực hiện như hướng dẫn dưới đây:

3.1. 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:

1) 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;

2) 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;

3) Thông tin cá nhân là thông tin trên mạng gắn với việc xác định danh tính một người cụ thể;

4) 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.

3.2. 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:

a) Hệ thống thư điện tử;

b) Hệ thống quản lý văn bản và điều hành;

c) Hệ thống họp, hội nghị truyền hình trực tuyến;

d) 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);

đ) 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:

a) Hệ thống thư điện tử;

b) Hệ thống quản lý văn bản và điều hành;

c) Hệ thống một cửa điện tử;

d) Hệ thống trang, cổng thông tin điện tử;

đ) Hệ thống cung cấp hoặc hỗ trợ cung cấp dịch vụ trực tuyến;

e) 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:

a) Mạng nội bộ, mạng diện rộng, mạng truyền số liệu chuyên dùng;

b) Hệ thống cơ sở dữ liệu, trung tâm dữ liệu, điện toán đám mây;

c) Hệ thống xác thực điện tử, chứng thực điện tử, chữ ký số;

d) 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:

a) Hệ thống điều khiển lập trình được (PLCs);

b) Hệ thống điều khiển phân tán (DCS);

c) Hệ thống giám sát và thu thập dữ liệu (SCADA).

Ngoài các hệ thống thông tin được phân loại như 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.

3.3. 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 85/2016/NĐ-CP từ Điều 7 đến Điều 11. Về cơ bản, việc áp dụng các tiêu chí xác định vào một hệ thống thông tin cụ thể có thể thực hiện như sau:

Trước hết cần xác định hệ thống thông tin cần xác định cấp độ. Đây là cơ sở để xác định loại thông tin hệ thống đó xử lý và loại hình của hệ thống thông tin đó.

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.

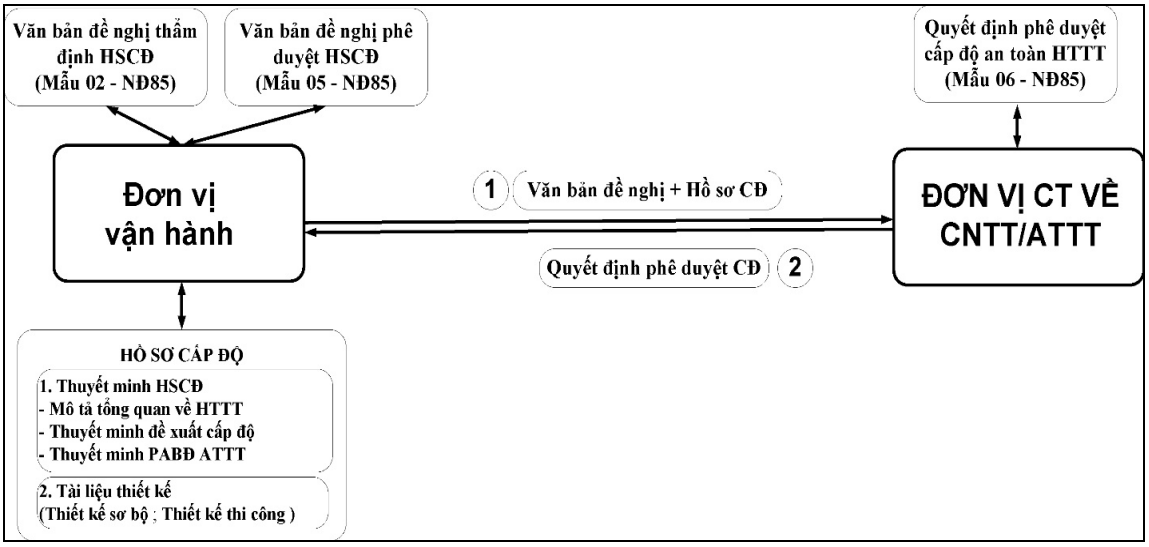
- Trường hợp hệ thống là hệ thống thông tin điều khiển công nghiệp trực tiếp phục vụ điều khiển, vận hành hoạt động bình thường của các công trình xây dựng cấp I theo phân cấp của pháp luật về xây dựng thì cấp độ đề xuất là cấp độ 4; Trường hợp hệ thống phục vụ điều khiển công trình xây dựng cấp đặc 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 và Thông tư 03/2017/TT-BTTTT.

Chương IV
QUY TRÌNH THẨM ĐỊNH, PHÊ DUYỆT

Thẩm quyền, quy trình, thủ tục xác định cấp độ an toàn hệ thống thông tin được quy định từ Điều 12 đến Điều 18 Nghị định 85/2016/NĐ-CP. Dưới đây là hướng dẫn chi tiết quy trình, thủ tục xác định cấp độ của hệ thống thông tin được đề xuất từ cấp độ 1 đến cấp độ 5.

4.1. Hệ thống thông tin đề xuất cấp độ 1 hoặc cấp độ 2



Hình 1: Hệ thống thông tin đề xuất cấp độ 1 hoặc cấp độ 2

Bước 1: Chuẩn bị HSĐXCĐ

Đơn vị vận hành hệ thống thông tin chuẩn bị HSĐXCĐ bao gồm các tài liệu sau:

1. Hồ sơ đề xuất cấp độ.

2. Văn bản đề nghị thẩm định HSĐXCĐ (Theo mẫu Mau02-ND85).

3. Văn bản đề nghị phê duyệt HSĐXCĐ (Theo mẫu Mau05-ND85).

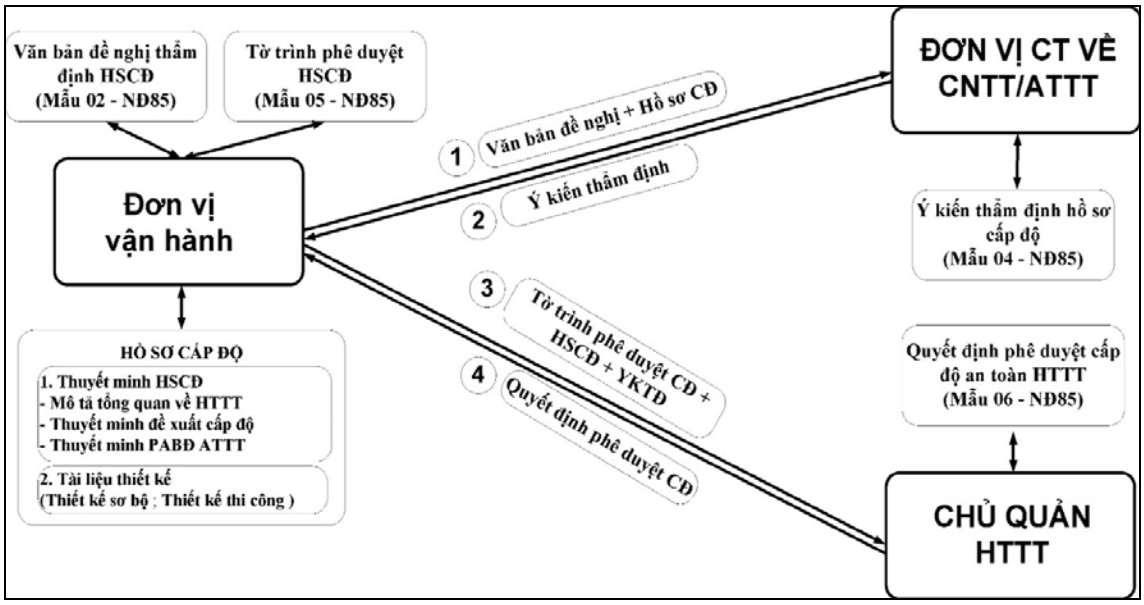
Bước 2: Thẩm định và phê duyệt HSĐXCĐ

1. Đơn vị vận hành hệ thống thông tin (ĐVVH) gửi hồ sơ đề xuất cấp độ tới đơn vị chuyên trách về CNTT/ATTT (ĐVCT) của Chủ quản hệ thống thông tin (CQHTTT) để lấy ý kiến thẩm định.

2. Đơn vị chuyên trách về CNTT/ATTT của CQHTTT thực hiện thẩm định HSĐXCĐ.

3. Trong vòng 15 ngày kể từ ngày nhận đủ hồ sơ hợp lệ, đơn vị chuyên trách về CNTT/ATTT có ý kiến thẩm định và phê duyệt HSĐXCĐ theo mẫu Mau06-ND85 và gửi báo cáo CQHTTT.

4.2. Hệ thống thông tin đề xuất cấp độ 3



Hình 2: Hệ thống thông tin đề xuất cấp độ 3

Bước 1: Chuẩn bị HSĐXCĐ

Đơn vị vận hành hệ thống thông tin chuẩn bị HSĐXCĐ bao gồm các tài liệu sau:

1. Thuyết minh Hồ sơ đề xuất cấp độ;

2. Văn bản đề nghị thẩm định HSĐXCĐ (Theo mẫu Mau02-ND85);

3. Văn bản đề nghị phê duyệt HSĐXCĐ (Theo mẫu Mau05-ND85).

Bước 2: Gửi xin ý kiến thẩm định của Đơn vị chuyên trách

1. ĐVVH gửi hồ sơ đề xuất cấp độ tới ĐVCT của CQHTTT để lấy ý kiến thẩm định.

2. ĐVCT thực hiện thẩm định hồ sơ đề xuất cấp độ.

3. Trong vòng 15 ngày kể từ ngày nhận đủ hồ sơ hợp lệ, ĐVCT có ý kiến thẩm định cho HSĐXCĐ theo mẫu Mau04-ND85.

Bước 3: Đề nghị phê duyệt HSĐXCĐ

Sau khi nhận được ý kiến thẩm định và hoàn thiện HSĐXCĐ theo ý kiến thẩm định, ĐVVH gửi HSĐXCĐ tới CQHTTT đề nghị phê duyệt HSĐXCĐ, Hồ sơ bao gồm:

- Tờ trình phê duyệt cấp độ (theo mẫu Mau05-ND85);

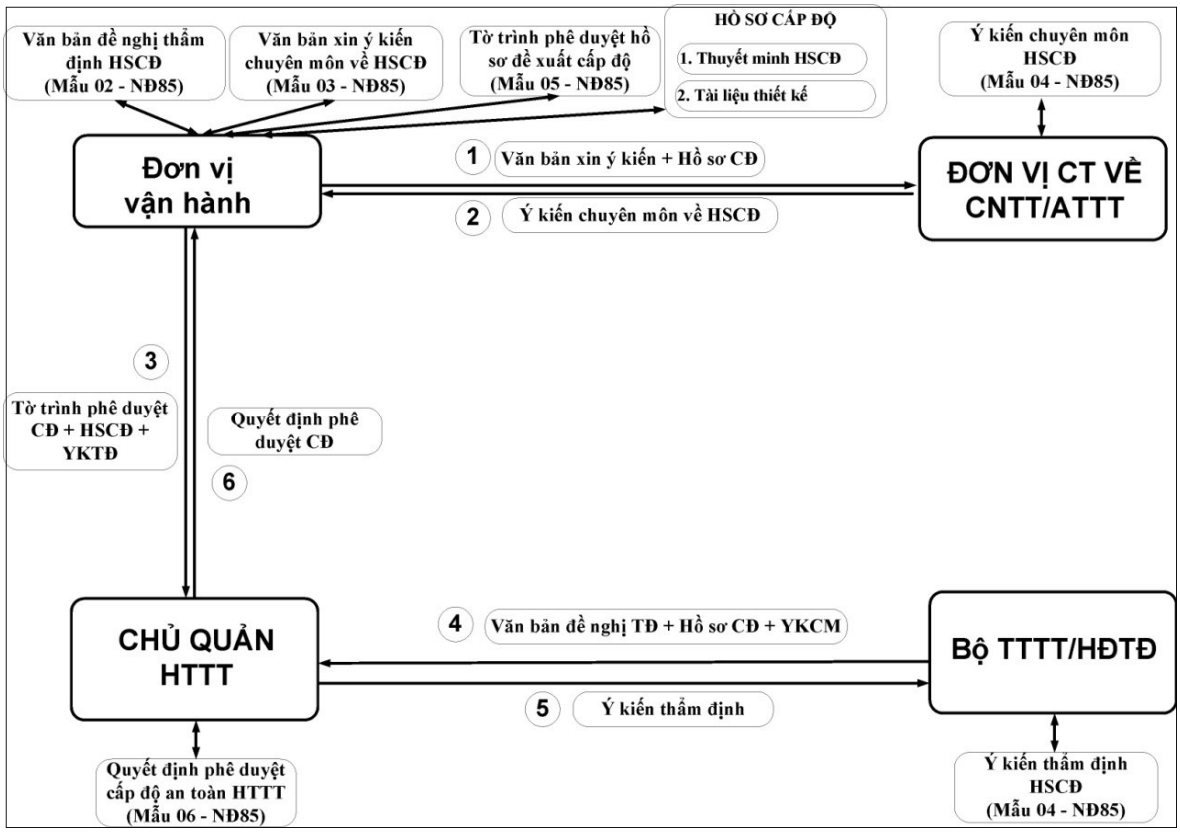
- Hồ sơ đề xuất cấp độ;

- Ý kiến thẩm định HSĐXCĐ.

Bước 4: Phê duyệt HSĐXCĐ

Căn cứ vào ý kiến thẩm định của ĐVCT, CQHTTT phê duyệt hoặc yêu cầu ĐVVH sửa đổi bổ sung HSĐXCĐ theo thẩm quyền. Trường hợp HSĐXCĐ đạt yêu cầu theo quy định, CQHTTT phê duyệt cấp độ an toàn hệ thống thông tin theo mẫu Mau06-ND85.

4.3. Hệ thống thông tin đề xuất cấp độ 4



Hình 3: Hệ thống thông tin đề xuất cấp độ 4

Bước 1: Chuẩn bị HSĐXCĐ

Đơn vị vận hành hệ thống thông tin chuẩn bị HSĐXCĐ bao gồm các tài liệu sau:

1. Thuyết minh Hồ sơ đề xuất cấp độ;

2. Văn bản đề nghị thẩm định HSĐXCĐ (Theo mẫu Mau02-ND85);

3. Văn bản đề nghị phê duyệt HSĐXCĐ (Theo mẫu Mau05-ND85).

Bước 2: Gửi xin ý kiến chuyên môn HSĐXCĐ

1. ĐVVH gửi hồ sơ đề xuất cấp độ tới ĐVCT của CQHTTT để lấy ý kiến chuyên môn.

2. ĐVCT của CQHTTT thực hiện kiểm tra hồ sơ đề xuất cấp độ.

3. Trong vòng 15 ngày kể từ ngày nhận đủ hồ sơ hợp lệ, ĐVCT của CQHTTT có ý kiến thẩm định cho HSĐXCĐ theo mẫu Mau04-ND85.

Bước 3: Đề nghị phê duyệt HSĐXCĐ

Sau khi nhận được ý kiến thẩm định và hoàn thiện HSĐXCĐ theo ý kiến thẩm định, ĐVVH gửi HSĐXCĐ tới CQHTTT đề nghị phê duyệt HSĐXCĐ, Hồ sơ bao gồm:

1. Các văn bản tại Bước 1;

2. Ý kiến chuyên môn của ĐVCT tại Bước 2.

Bước 4: Gửi xin ý kiến thẩm định của Bộ TT&TT

Sau khi nhận được HSĐXCĐ hợp lệ từ ĐVVH, CQHTTT gửi HSĐXCĐ về Bộ TT&TT đề nghị thẩm định.

Bước 5: Bộ TT&TT thẩm định HSĐXCĐ

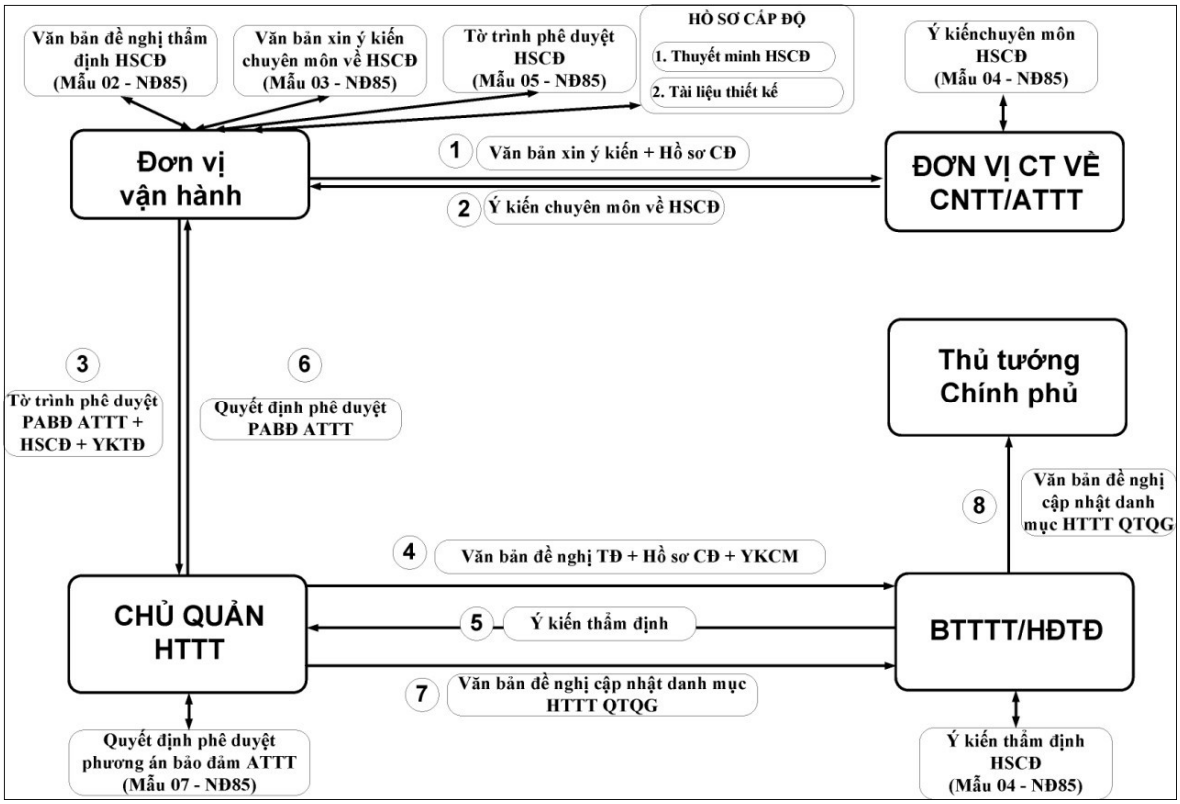
1. Bộ TT&TT lấy ý kiến bằng văn bản Bộ Quốc phòng, Bộ Công an để xin ý kiến thẩm định. Trong trường hợp cần thiết, Bộ TT&TT tổ chức Hội đồng thẩm định để có ý kiến thẩm định cho HSĐXCĐ.

2. Trong vòng 30 ngày kể từ ngày nhận đủ hồ sơ hợp lệ, Bộ TT&TT gửi CQHTTT ý kiến thẩm định theo mẫu Mau04-ND85.

Bước 6: Chủ quản HTTT phê duyệt HSĐXCĐ

Căn cứ vào ý kiến thẩm định của Bộ TT&TT, CQHTTT phê duyệt hoặc yêu cầu ĐVVH sửa đổi bổ sung HSĐXCĐ theo thẩm quyền. Trường hợp HSĐXCĐ đạt yêu cầu theo quy định, CQHTTT phê duyệt cấp độ an toàn hệ thống thông tin theo mẫu Mau06-ND85.

4.4. Hệ thống thông tin đề xuất cấp độ 5



Hình 4: Hệ thống thông tin đề xuất cấp độ 5

Bước 1: Chuẩn bị HSĐXCĐ

Đơn vị vận hành hệ thống thông tin chuẩn bị HSĐXCĐ bao gồm các tài liệu sau:

1. Thuyết minh Hồ sơ đề xuất cấp độ:

2. Văn bản đề nghị thẩm định HSĐXCĐ (Theo mẫu Mau02-ND85);

3. Văn bản xin ý kiến chuyên môn về HSĐXCĐ (Theo mẫu Mau03-ND85);

4. Văn bản đề nghị phê duyệt Phương án đảm bảo ATTT (Theo mẫu Mau05-ND85).

Bước 2: Gửi xin ý kiến chuyên môn HSĐXCĐ

1. ĐVVH gửi hồ sơ đề xuất cấp độ tới ĐVCT của CQHTTT để lấy ý kiến chuyên môn.

2. ĐVCT của CQHTTT thực hiện kiểm tra hồ sơ đề xuất cấp độ.

3. Trong vòng 15 ngày kể từ ngày nhận đủ hồ sơ hợp lệ, ĐVCT của CQHTTT có ý kiến thẩm định cho HSĐXCĐ theo mẫu Mau04-ND85.

Bước 3: Đề nghị phê duyệt HSĐXCĐ

Sau khi nhận được ý kiến thẩm định và hoàn thiện HSĐXCĐ theo ý kiến thẩm định, ĐVVH gửi HSĐXCĐ tới CQHTTT đề nghị phê duyệt HSĐXCĐ, Hồ sơ bao gồm:

1. Các văn bản tại Bước 1;

2. Ý kiến chuyên môn của ĐVCT tại Bước 2.

Bước 4: Gửi xin ý kiến thẩm định của Bộ TT&TT

Sau khi nhận được HSĐXCĐ hợp lệ từ ĐVVH, CQHTTT gửi HSĐXCĐ về Bộ TT&TT đề nghị thẩm định.

Bước 5: Bộ TT&TT thẩm định HSĐXCĐ

1. Bộ TT&TT lấy ý kiến bằng văn bản Bộ Quốc phòng, Bộ Công an để xin ý kiến thẩm định. Trong trường hợp cần thiết, Bộ TT&TT tổ chức Hội đồng thẩm định để có ý kiến thẩm định cho HSĐXCĐ.

2. Trong vòng 30 ngày kể từ ngày nhận đủ hồ sơ hợp lệ, Bộ TT&TT gửi CQHTTT ý kiến thẩm định theo mẫu Mau04-ND85.

Bước 6: Phê duyệt PABĐ ATTT

Căn cứ vào ý kiến thẩm định của Bộ TT&TT, CQHTTT phê duyệt hoặc yêu cầu ĐVVH sửa đổi bổ sung HSĐXCĐ theo thẩm quyền. Trường hợp HSĐXCĐ đạt yêu cầu theo quy định, CQHTTT phê duyệt phương án bảo đảm an toàn hệ thống thông tin theo mẫu Mau07-ND85.

Bước 7: Cập nhật danh mục HTTT Quan trọng Quốc gia (HTTT QTQG).

Sau khi phê duyệt phương án bảo đảm an toàn thông tin, CQHTTT gửi văn bản đề nghị Bộ TT&TT cập nhật danh mục Hệ thống thông tin quan trọng Quốc gia.

Bước 8: Trình Thủ tướng phê duyệt HTTT QTQG.

Bộ TT&TT chủ trì, phối hợp với Bộ Quốc phòng, Bộ Công an và bộ, ngành có liên quan trình Thủ tướng Chính phủ văn bản đề nghị cập nhật danh mục HTTT quan trọng quốc gia.

Chương V
HƯỚNG DẪN XÂY DỰNG HỒ SƠ ĐỀ XUẤT CẤP ĐỘ

HSĐXCĐ bao gồm hai loại tài liệu bản cứng: Tài liệu thuyết minh HSĐXCĐ và Tài liệu thiết kế hệ thống.

Trong đó, tài liệu thuyết minh HSĐXCĐ bao gồm các nội dung sau: (1) Thuyết minh tổng quan về hệ thống thông tin; (2) Thuyết minh đề xuất cấp độ an toàn hệ thống thông tin; (3) Thuyết minh phương án bảo đảm an toàn thông tin.

Khi xây dựng HSĐXCĐ cần lưu 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 HSĐXCĐ chung cho các hệ thống thông tin thành phần. Chỉ xây dựng HSĐXCĐ cho từng hệ thống riêng biệt trong trường hợp độc lập về hạ tầng, cơ chế quản lý và đơn vị vận hành. Xây dựng HSĐXCĐ theo hướng dẫn sau:

5.1. Thuyết minh tổng quan về hệ thống thông tin

5.1.1. Thông tin Chủ quản hệ thống thông tin

Cung cấp thông tin về Chủ quản hệ thống thông tin, bao gồm:

- Tên Tổ chức: Tổ chức 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.

5.1.2. Thông tin Đơn vị vận hành

Cung cấp thông tin về đơn vị vận hành hệ thống thông tin bao gồm:

- Tên Tổ chức: Tổ chức 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.

5.1.3. Mô tả phạm vi, quy mô của hệ thống

Mô tả thành phần các ứng dụng, dịch vụ và đối tượng cung cấp dịch vụ của Hệ thống. Lưu ý một hệ thống thông tin có thể bao gồm các hệ thống thông tin thành phần trong đó và mỗi thành phần đó cung cấp một ứng dụng/dịch vụ khác nhau.

5.1.4. Mô tả cấu trúc của hệ thống

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

a) 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.

b) 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 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/2016/NĐ-CP ngày 01/07/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ (Thông tư 03/2017/TT-BTTTT) thì việc mô tả cấu trúc của hệ thống thông tin đó được mô tả theo cấu trúc thực tế của hệ thống.

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.

5.2. Thuyết minh cấp độ đề xuất

5.2.1. Xác định hệ thống thông tin và cấp độ đề xuất

Hướng dẫn xác định hệ thống thông tin và cấp độ đề xuất tham khảo tại chương 3 của tài liệu này và lưu ý thêm như sau:

Khi xác định cấp độ, không cần thiết 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 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.

Lưu 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.

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

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 03/2017/TT-BTTTT. Bao gồm các nội dung:

a) 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;

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

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

d) 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;

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

5.3. Thuyết minh phương án bảo đảm an toàn thông tin

Đối với các yêu cầu an toàn về quản lý, các yêu cầu đã được đáp ứng, thuyết minh phương án sẽ chỉ ra các quy định theo yêu cầu được quy định tại quy chế/ chính sách bảo đảm an toàn thông tin nào. Trường hợp, các yêu cầu chưa đáp ứng thì thuyết minh sẽ đưa ra kế hoạch hoàn thiện quy chế, chính sách để đáp ứng các yêu cầu an toàn về quản lý như thế nào. Ví dụ: Thuyết minh này đưa ra kế hoạch hoàn thiện quy chế, chính sách để đáp ứng các yêu cầu an toàn về quản lý trong vòng 06 tháng, kể từ khi HSĐXCĐ được phê duyệt.

Đối với các yêu cầu kỹ thuật, các yêu cầu đã được đáp ứng, thuyết minh phương án sẽ mô tả các phương án, hiện trạng cấu hình và thiết lập hệ thống đã đáp ứng các yêu cầu đặt ra hay chưa? Trường hợp, các yêu cầu chưa đáp ứng thì thuyết minh sẽ đưa ra phương án, lộ trình để nâng cấp, điều chỉnh hệ thống nhằm đáp ứng các yêu cầu đặt ra. Ví dụ: Thuyết minh này đưa ra kế hoạch nâng cấp, điều chỉnh hệ thống để đáp ứng yêu cầu kỹ thuật trong vòng 18 tháng, kể từ khi HSĐXCĐ được phê duyệt.

Lưu ý: Trong trường hợp, Hệ thống thông tin gồm nhiều hệ thống thành phần khác nhau. Mỗi hệ thống thành phần được đề xuất cấp độ khác nhau. Đối với từng hệ thống thành phần khác nhau thì yêu cầu phương án bảo đảm an toàn thông tin theo cấp độ tương ứng. Do đó:

- Thuyết minh phương án bảo đảm an toàn thông tin về quản lý đưa ra các quy định liên quan đến con người và quy trình. Các yêu cầu quản lý ở cấp độ cao hơn khi được đáp ứng thì cũng đáp ứng các yêu cầu ở cấp độ thấp hơn. Do đó, thuyết minh phương án bảo đảm an toàn thông tin về quản lý được thuyết minh chung cho cả hệ thống lớn.

- Thuyết minh phương án bảo đảm an toàn thông tin về kỹ thuật liên quan đến việc thiết kế, thiết lập cấu hình hệ thống và liên quan trực tiếp đến đầu tư. Do đó, thuyết minh phương án về kỹ thuật được thuyết minh theo từng hệ thống thành phần theo cấp độ tương ứng theo nguyên tắc sau:

Đối với hạ tầng, thiết bị hệ thống, máy chủ dùng chung để bảo vệ nhiều hệ thống thành phần khác nhau, thì hạ tầng, thiết bị hệ thống, máy chủ đó phải được thiết kế, thiết lập để đáp ứng yêu cầu của hệ thống thành phần có cấp độ cao nhất.

Đối với hạ tầng, thiết bị hệ thống, máy chủ dùng riêng, độc lập đối với từng hệ thống thành phần, thì hạ tầng, thiết bị hệ thống, máy chủ đó phải được thiết kế, thiết lập để đáp ứng yêu cầu của hệ thống thành phần với cấp độ tương ứng nhằm bảo đảm tiết kiệm và hiệu quả.

Để thuyết minh chi tiết việc đáp ứng các yêu cầu an toàn quy định tại Thông tư số 03, cơ quan, tổ chức 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.

5.3.1. Thuyết minh phương án bảo đảm an toàn thông tin về quản lý:

Thuyết minh phương án bảo đảm an toàn thông tin về quản lý bao gồm các nội dung và theo cấu trúc sau:

1) Mục tiêu, nguyên tắc bảo đảm an toàn thông tin:

Mô tả mục tiêu, nguyên tắc bảo đảm an toàn thông tin của tổ chức.

2) Trách nhiệm bảo đảm an toàn thông tin.

Mô tả trách nhiệm bảo đảm an toàn thông tin của đơn vị chuyên trách về an toàn thông tin, các cán bộ làm về an toàn thông tin và các đối tượng thuộc phạm vi điều chỉnh của chính sách an toàn thông tin.

3) Phạm vi chính sách an toàn thông tin

Mô tả phạm vi chính sách, đối tượng áp dụng chính sách bảo đảm an toàn thông tin của tổ chức.

4) Tổ chức bảo đảm an toàn thông tin

Cung cấp thông tin về cơ cấu, tổ chức bảo đảm an toàn thông tin của tổ chức, bao gồm: Đơn vị chuyên trách về an toàn thông tin; Cơ chế, đầu mối phối hợp với cơ quan/tổ chức có thẩm quyền trong hoạt động bảo đảm an toàn thông tin.

Bảng ánh xạ giữa cấp độ và yêu cầu an toàn tương ứng trong TCVN 11930:2017.

Cấp độ đề xuất	**TCVN:11930**
Cấp độ 1	5.1.2
Cấp độ 2	6.1.2
Cấp độ 3	7.1.2
Cấp độ 4	8.1.2
Cấp độ 5	9.1.2

5) Bảo đảm nguồn nhân lực

Đưa ra chính sách/quy trình thực hiện quản lý bảo đảm nguồn nhân lực an toàn thông tin của tổ chức, bao gồm: Tuyển dụng cán bộ; quy chế/quy định bảo đảm an toàn thông tin trong quá trình làm việc và chấm dứt hoặc thay đổi công việc.

Bảng ánh xạ giữa cấp độ và yêu cầu an toàn tương ứng trong TCVN 11930:2017.

Cấp độ đề xuất	TCVN:11930
Cấp độ 1	5.1.3
Cấp độ 2	6.1.3
Cấp độ 3	7.1.3
Cấp độ 4	8.1.3
Cấp độ 5	9.1.3

6) Quản lý thiết kế, xây dựng hệ thống

Đưa ra chính sách/quy trình thực hiện quản lý thiết kế, xây dựng hệ thống của tổ chức, bao gồm: Thiết kế an toàn hệ thống thông tin; Phát triển phần mềm thuê khoán; Thử nghiệm và nghiệm thu hệ thống.

Bảng ánh xạ giữa cấp độ và yêu cầu an toàn tương ứng trong TCVN 11930:2017.

Cấp độ đề xuất	TCVN:11930
Cấp độ 1	5.1.4
Cấp độ 2	6.1.4
Cấp độ 3	7.1.4
Cấp độ 4	8.1.4
Cấp độ 5	9.1.4

7) Quản lý vận hành hệ thống

a) Quản lý an toàn mạng

Đưa ra chính sách/quy trình thực hiện quản lý an toàn hạ tầng mạng của tổ chức, bao gồm: Quản lý vận hành hoạt động bình thường của hệ thống; Cập nhật, sao lưu dự phòng và khôi phục hệ thống sau khi xảy ra sự cố; Truy cập và quản lý cấu hình hệ thống; Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống (cứng hóa) trước khi đưa vào vận hành, khai thác.

Bảng ánh xạ giữa cấp độ và yêu cầu an toàn tương ứng trong TCVN 11930:2017.

Cấp độ đề xuất	TCVN:11930
Cấp độ 1	5.1.5.1
Cấp độ 2	6.1.5.1
Cấp độ 3	7.1.5.1
Cấp độ 4	8.1.5.1
Cấp độ 5	9.1.5.1

b) Quản lý an toàn máy chủ và ứng dụng

Đưa ra chính sách/quy trình thực hiện quản lý an toàn máy chủ và ứng dụng của tổ chức, bao gồm: Quản lý vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ; Truy cập mạng của máy chủ; Truy cập và quản trị máy chủ và ứng dụng; Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố; Cài đặt, gỡ bỏ hệ điều hành, dịch vụ, phần mềm trên hệ thống; Kết nối và gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống; Cấu hình tối ưu và tăng cường bảo mật cho hệ thống máy chủ trước khi đưa vào vận hành, khai thác.

Bảng ánh xạ giữa cấp độ và yêu cầu an toàn tương ứng trong TCVN 11930:2017.

Cấp độ đề xuất	**TCVN:11930**
Cấp độ 1	5.1.5.2
Cấp độ 2	6.1.5.2
Cấp độ 3	7.1.5.2
Cấp độ 4	8.1.5.2
Cấp độ 5	9.1.5.2

c) Quản lý an toàn dữ liệu

Đưa ra chính sách/quy trình thực hiện quản lý an toàn dữ liệu của tổ chức, bao gồm: Yêu cầu an toàn đối với phương pháp mã hóa; Phân loại, quản lý và sử dụng khóa bí mật và dữ liệu mã hóa; Cơ chế mã hóa và kiểm tra tính nguyên vẹn của dữ liệu; Trao đổi dữ liệu qua môi trường mạng và phương tiện lưu trữ; Sao lưu dự phòng và khôi phục dữ liệu; Cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ.

Bảng ánh xạ giữa cấp độ và yêu cầu an toàn tương ứng trong TCVN 11930:2017.

Cấp độ đề xuất	**TCVN:11930**
Cấp độ 1	5.1.5.3
Cấp độ 2	6.1.5.3
Cấp độ 3	7.1.5.3
Cấp độ 4	8.1.5.3
Cấp độ 5	9.1.5.3

d) Quản lý an toàn thiết bị đầu cuối

Đưa ra chính sách/quy trình thực hiện quản lý an toàn thiết bị đầu cuối của tổ chức, bao gồm: Quản lý vận hành hoạt động bình thường cho thiết bị đầu cuối; Kết nối, truy cập và sử dụng thiết bị đầu cuối từ xa; Cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống; Cấu hình tối ưu và tăng cường bảo mật cho máy tính người sử dụng; Kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin cho thiết bị đầu cuối.

Bảng ánh xạ giữa cấp độ và yêu cầu an toàn tương ứng trong TCVN 11930:2017.

Cấp độ đề xuất	TCVN:11930
Cấp độ 1	Không yêu cầu
Cấp độ 2	6.1.5.5
Cấp độ 3	7.1.5.4
Cấp độ 4	8.1.5.4
Cấp độ 5	9.1.5.4

đ) Quản lý phòng chống phần mềm độc hại

Đưa ra chính sách/quy trình thực hiện quản lý phòng chống phần mềm độc hại của tổ chức, bao gồm: Cài đặt, cập nhật, sử dụng phần mềm phòng chống mã độc; Cài đặt, sử dụng phần mềm trên máy tính, thiết bị di động và việc truy cập các trang thông tin trên mạng; Gửi nhận tập tin qua môi trường mạng và các phương tiện lưu trữ di động; Thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; Kiểm tra và xử lý phần mềm độc hại.

Bảng ánh xạ giữa cấp độ và yêu cầu an toàn tương ứng trong TCVN 11930:2017.

Cấp độ đề xuất	TCVN:11930
Cấp độ 1	Không yêu cầu
Cấp độ 2	Không yêu cầu
Cấp độ 3	7.1.5.5
Cấp độ 4	8.1.5.5
Cấp độ 5	9.1.5.5

e) Quản lý giám sát an toàn hệ thống thông tin

Đưa ra chính sách/quy trình thực hiện quản lý phòng chống phần mềm độc hại của tổ chức, bao gồm: Quản lý vận hành hoạt động bình thường của hệ thống giám sát; Đối tượng giám sát bao gồm; Kết nối và gửi nhật ký hệ thống; Truy cập và quản trị hệ thống giám sát; Loại thông tin cần được giám sát; Lưu trữ và bảo vệ thông tin giám sát; Theo dõi, giám sát và cảnh báo sự cố; Bố trí nguồn lực và tổ chức giám sát.

Bảng ánh xạ giữa cấp độ và yêu cầu an toàn tương ứng trong TCVN 11930:2017.

Cấp độ đề xuất	TCVN:11930
Cấp độ 1	Không yêu cầu
Cấp độ 2	Không yêu cầu
Cấp độ 3	7.1.5.6
Cấp độ 4	8.1.5.6
Cấp độ 5	9.1.5.6

g) Quản lý điểm yếu an toàn thông tin

Đưa ra chính sách/quy trình thực hiện quản lý điểm yếu an toàn thông tin của tổ chức, bao gồm: Quản lý thông tin các thành phần có trong hệ thống có khả năng tồn tại điểm yếu an toàn thông tin; Quản lý, cập nhật nguồn cung cấp điểm yếu an toàn thông tin; Phân nhóm và mức độ của điểm yếu; Cơ chế phối hợp với các nhóm chuyên gia; Kiểm tra, đánh giá và xử lý điểm yếu an toàn thông tin trước khi đưa hệ thống vào sử dụng; Quy trình khôi phục lại hệ thống.

Bảng ánh xạ giữa cấp độ và yêu cầu an toàn tương ứng trong TCVN 11930:2017.

Cấp độ đề xuất	**TCVN:11930**
Cấp độ 1	Không yêu cầu
Cấp độ 2	Không yêu cầu
Cấp độ 3	7.1.5.7
Cấp độ 4	8.1.5.7
Cấp độ 5	9.1.5.7

h) Quản lý sự cố an toàn thông tin

Đưa ra chính sách/quy trình thực hiện quản lý sự cố an toàn thông tin của tổ chức, bao gồm: Phân nhóm sự cố an toàn thông tin; Phương án tiếp nhận, phát hiện, phân loại và xử lý thông tin; Kế hoạch ứng phó sự cố an toàn thông tin; Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin; Quy trình ứng cứu sự cố an toàn thông tin thông thường; Quy trình ứng cứu sự cố an toàn thông tin nghiêm trọng; Cơ chế phối hợp trong việc xử lý, khắc phục sự cố an toàn thông tin; Diễn tập phương án xử lý sự cố an toàn thông tin.

Bảng ánh xạ giữa cấp độ và yêu cầu an toàn tương ứng trong TCVN 11930:2017.

Cấp độ đề xuất	**TCVN:11930**
Cấp độ 1	Không yêu cầu
Cấp độ 2	6.1.5.4
Cấp độ 3	7.1.5.8
Cấp độ 4	8.1.5.8
Cấp độ 5	9.1.5.8

i) Quản lý an toàn người sử dụng đầu cuối

Đưa ra chính sách/quy trình thực hiện quản lý an toàn người sử dụng đầu cuối của tổ chức, bao gồm: Quản lý truy cập, sử dụng tài nguyên nội bộ; Quản lý truy cập mạng và tài nguyên trên Internet; Cài đặt và sử dụng máy tính an toàn.

Bảng ánh xạ giữa cấp độ và yêu cầu an toàn tương ứng trong TCVN 11930:2017.

Cấp độ đề xuất	TCVN:11930
Cấp độ 1	Không yêu cầu
Cấp độ 2	6.1.5.5
Cấp độ 3	7.1.5.9
Cấp độ 4	8.1.5.9
Cấp độ 5	9.1.5.9

5.3.2. Thuyết minh phương án bảo đảm an toàn thông tin về kỹ thuật

Yêu cầu an toàn cơ bản trong Thông tư 03/2017/TT-BTTTT và tiêu chuẩn quốc gia TCVN:11930 là yêu cầu cơ bản và phù hợp với loại hình hệ thống thông tin trong các cơ quan, tổ chức nhà nước. Do đó, đối với các hệ thống thông tin có đặc thù riêng, 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, một số hệ thống thông tin không có kết nối Internet, thì không phải thuyết minh phương án phòng chống DDoS hay thiết kế vùng mạng DMZ…

Lưu 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 hướng dẫn sau:

1) Bảo đảm an toàn mạng

a) Thiết kế hệ thống

- Liệt kê, mô tả thiết kế các vùng mạng trong hệ thống theo chức năng, các vùng mạng.

- Thuyết minh phương án thiết kế bảo đảm các yêu cầu tương ứng theo từng cấp độ, cụ thể như sau:

+ Phương án quản lý truy cập, quản trị hệ thống từ xa an toàn:

Mô tả thiết kế hệ thống mạng sử dụng thiết bị chuyên dụng hay thiết lập cấu hình chức năng bảo mật trên hệ thống hoặc phương án tương đương khác nếu có

để bảo đảm việc truy cập, quản trị hệ thống từ xa an toàn. Ví dụ sử dụng thiết bị VPN chuyên dụng hay cấu hình chức năng VPN trên thiết bị tường lửa…

+ Phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập:

Mô tả thiết kế hệ thống mạng sử dụng thiết bị tường lửa hoặc thiết bị có chức năng tương đương để quản lý truy cập và phòng chống xâm nhập giữa các vùng mạng. Lưu ý mô tả ngắn gọn các chức năng mà phương án cung cấp để quản lý truy cập và phòng chống xâm nhập giữa các vùng mạng.

+ Phương án cân bằng tải, dự phòng nóng cho các thiết bị mạng:

Mô tả phương án thiết kế và triển khai các thiết bị mạng trong hệ thống để thực hiện chức năng cân bằng tải, dự phòng nóng. Ví dụ: mô tả các thiết bị mạng được kết nối với nhau thế nào và được cấu hình HA hay AA…

+ Phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu:

Mô tả phương án sử dụng thiết bị chuyên dụng như tường lửa cơ sở dữ liệu hay phương án tương đương để bảo đảm an toàn cho máy chủ cơ sở dữ liệu. Lưu ý mô tả ngắn gọn các chức năng mà phương án cung cấp để bảo đảm an toàn cho máy chủ cơ sở dữ liệu.

+ Có phương án chặn lọc phần mềm độc hại trên môi trường mạng:

Mô tả phương án sử dụng thiết bị chuyên dụng hay chức năng trên thiết bị tường lửa hoặc phương án tương đương để phát hiện và ngăn chặn các hành vi mã độc trên môi trường mạng.

+ Phương án phòng chống tấn công từ chối dịch vụ:

Mô tả phương án sử dụng giải pháp chuyên dụng hay thuê dịch vụ hoặc phương án tương đương khác để phòng chống tấn công từ chối dịch vụ cho hệ thống (chỉ yêu cầu đối với các hệ thống có kết nối mạng Internet). Lưu ý cần mô tả ngắn gọn chức năng và năng lực xử lý tấn công từ chối dịch vụ của phương án sử dụng.

+ Phương án giám sát hệ thống thông tin tập trung:

Mô tả phương án sử dụng giải pháp chuyên dụng (ArcSight, Splunk, QRadar, LogRhythm) hay giải pháp tương đương khác để thực hiện giám sát hệ thống thông tin tập trung. Lưu ý mô tả ngắn gọn chức năng và năng lực xử lý của hệ thống giám sát tập trung.

+ Phương án giám sát an toàn hệ thống thông tin tập trung:

Mô tả phương án sử dụng giải pháp chuyên dụng (HP OpenView, Solarwinds…) hay giải pháp tương đương khác (Cacti, Nagios, MRTG…) để thực hiện giám sát hoạt

động của hệ thống mạng, bảo đảm tính sẵn sàng của hệ thống. Lưu ý mô tả ngắn gọn chức năng giám sát mà giải pháp cung cấp để đáp ứng yêu cầu.

+ Phương án quản lý sao lưu dự phòng tập trung:

Mô tả phương án quản lý sao lưu dự phòng tập trung sử dụng giải pháp chuyên dụng hoặc giải pháp tương đương sử dụng các giải pháp như SAN, NAS…Lưu ý mô tả ngắn gọn thông tin về giải pháp sử dụng và năng lực của giải pháp.

+ Phương án quản lý phần mềm phòng chống mã độc trên các máy chủ/máy tính người dùng tập trung:

Mô tả phương án quản lý tập trung các phần mềm phòng chống độc hại được cài đặt trên các máy tính /máy chủ gửi sử dụng thông qua một máy chủ quản lý tập trung. Lưu ý mô tả thông tin ngắn gọn, bao gồm thông tin về giải pháp sử dụng, năng lực và chức năng của giải pháp cung cấp để đáp ứng yêu cầu.

+ Phương án phòng, chống thất thoát dữ liệu:

Mô tả phương án phòng, chống thất thoát dữ liệu sử dụng trong hệ thống. Lưu ý mô tả thông tin ngắn gọn, bao gồm thông tin về giải pháp sử dụng, năng lực và chức năng của giải pháp cung cấp để đáp ứng yêu cầu.

+ 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);

+ Phương án bảo đảm an toàn cho mạng không dây:

Mô tả phương án bảo mật cho mạng không dây sử dụng giải pháp chuyên dụng hoặc việc thiết lập cấu hình bảo mật trên hệ thống để bảo đảm an toàn cho mạng không dây. Lưu ý mô tả thông tin ngắn gọn, bao gồm thông tin về giải pháp sử dụng, năng lực và chức năng của giải pháp cung cấp để đáp ứng yêu cầu.

+ Phương án quản lý tài khoản đặc quyền:

Mô tả phương án quản lý tài khoản đặc quyền cho phép quản lý tập trung việc xác thực, phân quyền, giám sát hành vi và các chức năng bảo mật khác để quản lý các tài khoản quản trị trong hệ thống. Lưu ý mô tả thông tin ngắn gọn, bao gồm thông tin về giải pháp sử dụng, năng lực và chức năng của giải pháp cung cấp để đáp ứng yêu cầu.

+ Phương án dự phòng hệ thống ở vị trí địa lý khác nhau:

Cung cấp thông tin ngắn gọn về hệ thống dự phòng như: ở vị trí địa lý nào? Chức năng chính của hệ thống dự phòng và nguyên lý hoạt động cơ bản của hệ thống để thực hiện chức năng dự phòng.

+ Phương án dự phòng cho kết nối mạng giữa hệ thống chính và hệ thống dự phòng:

Mô tả phương án kết nối mạng giữa hệ thống chính và hệ thống dự phòng để thực hiện đồng bộ dữ liệu và dự phòng nóng khi hệ thống chính xảy ra sự cố.

b) Kiểm soát truy cập từ bên ngoài mạng

Mô tả việc quản lý truy cập từ các mạng bên ngoài theo chiều đi vào hệ thống tới các máy chủ dịch vụ bên trong mạng, bao gồm: Các dịch vụ/ứng dụng cho phép từ truy cập từ bên ngoài; Thời gian mất kết nối; Phân quyền truy cập; Giới hạn kết nối; Thiết lập chính sách ưu tiên. Phương án cần mô tả chính sách đó được thiết lập trên thiết bị hệ thống nào.

Bảng ánh xạ giữa cấp độ và yêu cầu an toàn tương ứng trong TCVN 11930:2017.

Cấp độ đề xuất	**TCVN:11930**
Cấp độ 1	5.2.1.2
Cấp độ 2	6.2.1.2
Cấp độ 3	7.2.1.2
Cấp độ 4	8.2.1.2
Cấp độ 5	9.2.1.2

c) Kiểm soát truy cập từ bên trong mạng

Mô tả phương án quản lý truy cập từ các máy tính/máy chủ bên trong mạng theo chiều đi ra các mạng bên ngoài và các mạng khác bên trong mạng, bao gồm: Các ứng dụng/dịch vụ nào được truy cập; Quản lý truy cập theo địa chỉ thiết bị; phương án ưu tiên truy cập. Phương án cần mô tả chính sách đó được thiết lập trên thiết bị hệ thống nào.

Bảng ánh xạ giữa cấp độ và yêu cầu an toàn tương ứng trong TCVN 11930:2017.

Cấp độ đề xuất	**TCVN:11930**
Cấp độ 1	Không yêu cầu
Cấp độ 2	6.2.1.3
Cấp độ 3	7.2.1.3
Cấp độ 4	8.2.1.3
Cấp độ 5	9.2.1.3

d) Nhật ký hệ thống

Mô tả phương án quản lý nhật ký hệ thống (log) trên các thiết bị hệ thống về bật chức năng ghi log; thông tin ghi log; thời gian, dung lượng ghi log; quản lý log.

Bảng ánh xạ giữa cấp độ và yêu cầu an toàn tương ứng trong TCVN 11930:2017.

Cấp độ đề xuất	TCVN:11930
Cấp độ 1	5.2.1.3
Cấp độ 2	6.2.1.4
Cấp độ 3	7.2.1.4
Cấp độ 4	8.2.1.4
Cấp độ 5	9.2.1.4

Lưu ý: Đối với hệ thống đã đưa vào vận hành khai thác cần liệt kê các thiết bị trong hệ thống đã được thiết lập cấu hình nhật ký hệ thống và chỉ rõ đã đáp ứng được các yêu cầu an toàn nào.

đ) Phòng chống xâm nhập

Mô tả phương án triển khai/thiết lập cấu hình của thiết bị phòng, chống xâm nhập IDS/IPS hoặc chức năng IDS/IPS trên thiết bị tường lửa có trong hệ thống nhằm đáp ứng yêu cầu an toàn.

Bảng ánh xạ giữa cấp độ và yêu cầu an toàn tương ứng trong TCVN 11930:2017.

Cấp độ đề xuất	TCVN:11930
Cấp độ 1	5.2.1.4
Cấp độ 2	6.2.1.5
Cấp độ 3	7.2.1.5
Cấp độ 4	8.2.1.5
Cấp độ 5	9.2.1.5

Lưu ý: Đối với hệ thống đã đưa vào vận hành khai thác cần làm rõ việc triển khai chức năng phòng chống xâm nhập trên thiết bị nào, đặt tại vị trí nào trong hệ thống.

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

Mô tả phương án triển khai/thiết lập cấu hình của thiết bị để thực hiện chức năng phòng chống phần mềm độc hại trên môi trường mạng đáp ứng yêu cầu an toàn.

Bảng ánh xạ giữa cấp độ và yêu cầu an toàn tương ứng trong TCVN 11930:2017.

Cấp độ đề xuất	TCVN:11930
Cấp độ 1	Không yêu cầu
Cấp độ 2	Không yêu cầu
Cấp độ 3	7.2.1.6
Cấp độ 4	8.2.1.6
Cấp độ 5	9.2.1.6

Lưu ý: Đối với hệ thống đã đưa vào vận hành khai thác cần làm rõ việc triển khai chức năng phòng chống phần mềm độc hại trên môi trường mạng trên thiết bị nào, đặt tại vị trí nào trong hệ thống.

g) Bảo vệ thiết bị hệ thống

Mô tả phương án triển khai/thiết lập cấu hình chức năng bảo mật trên các thiết bị có trong hệ thống nhằm bảo đảm bảo đảm an toàn cho thiết bị trong quá trình sử dụng và quản lý vận hành.

Bảng ánh xạ giữa cấp độ và yêu cầu an toàn tương ứng trong TCVN 11930:2017.

Cấp độ đề xuất	TCVN:11930
Cấp độ 1	5.2.1.5
Cấp độ 2	6.2.1.6
Cấp độ 3	7.2.1.7
Cấp độ 4	8.2.1.7
Cấp độ 5	9.2.1.7

Lưu ý: Đối với hệ thống đã đưa vào vận hành khai thác cần liệt kê các thiết bị trong hệ thống đã được thiết lập chức năng bảo mật và chỉ rõ đã đáp ứng được các yêu cầu an toàn này.

2) Bảo đảm an toàn máy chủ

a) Xác thực

Mô tả việc cấu trình/thiết lập chính sách xác thực trên máy chủ để bảo đảm việc xác thực khi đăng nhập vào máy chủ an toàn.

Bảng ánh xạ giữa cấp độ và yêu cầu an toàn tương ứng trong TCVN 11930:2017.

Cấp độ đề xuất	TCVN:11930
Cấp độ 1	5.2.2.1
Cấp độ 2	6.2.2.1
Cấp độ 3	7.2.2.1
Cấp độ 4	8.2.2.1
Cấp độ 5	9.2.2.1

Lưu ý: Đối với hệ thống hệ thống thông tin đã đưa vào vận hành khai thác cần liệt kê các máy chủ có trong hệ thống đã được thiết lập chính sách xác thực và chỉ rõ đã đáp ứng các yêu cầu an toàn nào.

b) Kiểm soát truy cập

Mô tả việc cấu trình/thiết lập chính sách kiểm soát truy cập trên máy chủ để bảo đảm việc truy cập, sử dụng máy chủ an toàn sau khi đăng nhập thành công.

Bảng ánh xạ giữa cấp độ và yêu cầu an toàn tương ứng trong TCVN 11930:2017.

Cấp độ đề xuất	TCVN:11930
Cấp độ 1	5.2.2.1
Cấp độ 2	6.2.2.1
Cấp độ 3	7.2.2.1
Cấp độ 4	8.2.2.1
Cấp độ 5	9.2.2.1

Lưu ý: Đối với hệ thống hệ thống thông tin đã đưa vào vận hành khai thác cần liệt kê các máy chủ có trong hệ thống đã được thiết lập chính sách kiểm soát truy cập và chỉ rõ đã đáp ứng các yêu cầu an toàn nào.

c) Nhật ký hệ thống

Mô tả phương án quản lý nhật ký hệ thống (log) trên các máy chủ về: Bật chức năng ghi log; Thông tin ghi log; Thời gian, Dung lượng ghi log; Quản lý log.

Bảng ánh xạ giữa cấp độ và yêu cầu an toàn tương ứng trong TCVN 11930:2017.

Cấp độ đề xuất	TCVN:11930
Cấp độ 1	5.2.2.3
Cấp độ 2	6.2.2.3
Cấp độ 3	7.2.2.3
Cấp độ 4	8.2.2.3
Cấp độ 5	9.2.2.3

Lưu ý: Đối với hệ thống đã đưa vào vận hành khai thác cần liệt kê các máy chủ trong hệ thống đã được thiết lập cấu hình nhật ký hệ thống và chỉ rõ đã đáp ứng được các yêu cầu an toàn nào.

d) Phòng chống xâm nhập

Mô tả việc cấu trình/thiết lập cấu hình bảo mật trên máy chủ để bảo bảo vệ tấn công xâm nhập từ bên ngoài.

Bảng ánh xạ giữa cấp độ và yêu cầu an toàn tương ứng trong TCVN 11930:2017.

Cấp độ đề xuất	TCVN:11930
Cấp độ 1	5.2.2.4
Cấp độ 2	6.2.2.4
Cấp độ 3	7.2.2.4
Cấp độ 4	8.2.2.4
Cấp độ 5	9.2.2.4

Lưu ý: Đối với hệ thống đã đưa vào vận hành khai thác cần liệt kê các máy chủ trong hệ thống đã được thiết lập cấu hình bảo mật và chỉ rõ đã đáp ứng được các yêu cầu an toàn nào.

đ) Phòng chống phần mềm độc hại

Mô tả việc cấu trình/thiết lập cấu hình bảo mật trên máy chủ về: Cài đặt phần mềm phòng chống mã độc; Dò quét mã độc; Xử lý mã độc; Quản lý tập trung phần mềm phòng chống mã độc...để phòng chống mã độc cho máy chủ.

Bảng ánh xạ giữa cấp độ và yêu cầu an toàn tương ứng trong TCVN 11930:2017.

Cấp độ đề xuất	**TCVN:11930**
Cấp độ 1	5.2.2.5
Cấp độ 2	6.2.2.5
Cấp độ 3	7.2.2.5
Cấp độ 4	8.2.2.5
Cấp độ 5	9.2.2.5

Lưu ý: Đối với hệ thống đã đưa vào vận hành khai thác cần liệt kê các máy chủ trong hệ thống đã được thiết lập cấu hình phòng chống phần mềm độc hại và chỉ rõ đã đáp ứng được các yêu cầu an toàn nào.

e) Xử lý máy chủ khi chuyển giao

Mô tả phương án xóa sạch dữ liệu; sao lưu dự phòng dữ liệu khi chuyển giao hoặc thay đổi mục đích sử dụng.

Bảng ánh xạ giữa cấp độ và yêu cầu an toàn tương ứng trong TCVN 11930:2017.

Cấp độ đề xuất	**TCVN:11930**
Cấp độ 1	Không yêu cầu
Cấp độ 2	6.2.2.6
Cấp độ 3	7.2.2.6
Cấp độ 4	8.2.2.6
Cấp độ 5	9.2.2.6

3) Bảo đảm an toàn ứng dụng

a) Xác thực

Mô tả việc cấu trình/thiết lập chính sách xác thực trên ứng dụng để bảo đảm việc xác thực khi đăng nhập vào máy chủ an toàn.

Bảng ánh xạ giữa cấp độ và yêu cầu an toàn tương ứng trong TCVN 11930:2017.

Cấp độ đề xuất	TCVN:11930
Cấp độ 1	5.2.3.1
Cấp độ 2	6.2.3.1
Cấp độ 3	7.2.3.1
Cấp độ 4	8.2.3.1
Cấp độ 5	9.2.3.1

Lưu ý: Đối với hệ thống hệ thống thông tin đã đưa vào vận hành khai thác cần liệt kê các ứng dụng đã được thiết lập chính sách xác thực và chỉ rõ đã đáp ứng các yêu cầu an toàn nào.

b) Kiểm soát truy cập

Mô tả việc cấu trình/thiết lập chính sách kiểm soát truy cập trên ứng dụng để bảo đảm việc truy cập, sử dụng ứng dụng an toàn sau khi đăng nhập thành công.

Bảng ánh xạ giữa cấp độ và yêu cầu an toàn tương ứng trong TCVN 11930:2017.

Cấp độ đề xuất	TCVN:11930
Cấp độ 1	5.2.3.2
Cấp độ 2	6.2.3.2
Cấp độ 3	7.2.3.2
Cấp độ 4	8.2.3.2
Cấp độ 5	9.2.3.2

Lưu ý: Đối với hệ thống hệ thống thông tin đã đưa vào vận hành khai thác cần liệt kê các ứng dụng đã được thiết lập chính sách kiểm soát truy cập và chỉ rõ đã đáp ứng các yêu cầu an toàn nào.

c) Nhật ký hệ thống

Mô tả phương án quản lý nhật ký hệ thống (log) trên các ứng dụng về: Bật chức năng ghi log; Thông tin ghi log; Thời gian, dung lượng ghi log; Quản lý log.

Bảng ánh xạ giữa cấp độ và yêu cầu an toàn tương ứng trong TCVN 11930:2017.

Cấp độ đề xuất	TCVN:11930
Cấp độ 1	5.2.2.3
Cấp độ 2	6.2.2.3
Cấp độ 3	7.2.2.3
Cấp độ 4	8.2.2.3
Cấp độ 5	9.2.2.3

Lưu ý: Đối với hệ thống đã đưa vào vận hành khai thác cần liệt kê các máy chủ trong hệ thống đã được thiết lập cấu hình nhật ký hệ thống và chỉ rõ đã đáp ứng được các yêu cầu an toàn nào.

d) Bảo mật thông tin liên lạc

Mô tả phương án mã hóa và sử dụng giao thức mạng hoặc kênh kết nối mạng an toàn khi trao đổi dữ liệu qua môi trường mạng.

Bảng ánh xạ giữa cấp độ và yêu cầu an toàn tương ứng trong TCVN 11930:2017.

Cấp độ đề xuất	TCVN:11930
Cấp độ 1	Không yêu cầu
Cấp độ 2	Không yêu cầu
Cấp độ 3	7.2.3.4
Cấp độ 4	8.2.3.4
Cấp độ 5	9.2.3.4

đ) Chống chối bỏ

Mô tả phương án sử dụng và bảo vệ chữ ký số để bảo vệ tính bí mật và chống chối bỏ khi gửi/nhận thông tin quan trọng qua mạng.

Bảng ánh xạ giữa cấp độ và yêu cầu an toàn tương ứng trong TCVN 11930:2017.

Cấp độ đề xuất	TCVN:11930
Cấp độ 1	Không yêu cầu
Cấp độ 2	Không yêu cầu
Cấp độ 3	7.2.3.5
Cấp độ 4	8.2.3.5
Cấp độ 5	9.2.3.5

e) An toàn ứng dụng và mã nguồn

Mô tả phương án cấu hình/thiết lập chức năng bảo mật cho ứng dụng và phương án bảo vệ mã nguồn ứng dụng.

Bảng ánh xạ giữa cấp độ và yêu cầu an toàn tương ứng trong TCVN 11930:2017.

Cấp độ đề xuất	TCVN:11930
Cấp độ 1	Không yêu cầu
Cấp độ 2	6.2.3.4
Cấp độ 3	7.2.3.6
Cấp độ 4	8.2.3.6
Cấp độ 5	9.2.3.6

Lưu ý: Đối với hệ thống đã đưa vào vận hành khai thác cần liệt kê các ứng dụng đã được thiết lập cấu hình và chỉ rõ đã đáp ứng được các yêu cầu an toàn nào.

4) Bảo đảm an toàn dữ liệu

a) Nguyên vẹn dữ liệu

Mô tả phương án lưu trữ, quản lý thay đổi, khôi phục dữ liệu bảo đảm tính nguyên vẹn của dữ liệu.

Bảng ánh xạ giữa cấp độ và yêu cầu an toàn tương ứng trong TCVN 11930:2017.

Cấp độ đề xuất	TCVN:11930
Cấp độ 1	Không yêu cầu
Cấp độ 2	Không yêu cầu
Cấp độ 3	7.2.4.1
Cấp độ 4	8.2.4.1
Cấp độ 5	9.2.4.1

b) Bảo mật dữ liệu

Mô tả phương án lưu trữ, quản lý thay đổi, khôi phục dữ liệu bảo đảm tính bí mật của dữ liệu.

Bảng ánh xạ giữa cấp độ và yêu cầu an toàn tương ứng trong TCVN 11930:2017.

Cấp độ đề xuất	TCVN:11930
Cấp độ 1	Không yêu cầu
Cấp độ 2	6.2.4.1
Cấp độ 3	7.2.4.2
Cấp độ 4	8.2.4.2
Cấp độ 5	9.2.4.2

c) Sao lưu dự phòng

Mô tả phương án sao lưu dự phòng dữ liệu: Các thông tin yêu cầu sao lưu dự phòng; Phân loại dữ liệu sao lưu dự phòng; Hệ thống sao lưu dự phòng…

Bảng ánh xạ giữa cấp độ và yêu cầu an toàn tương ứng trong TCVN 11930:2017.

Cấp độ đề xuất	TCVN:11930
Cấp độ 1	5.2.4.1
Cấp độ 2	6.2.4.2
Cấp độ 3	7.2.4.3
Cấp độ 4	8.2.4.3
Cấp độ 5	9.2.4.3

Chương VI
HƯỚNG DẪN THẨM ĐỊNH HỒ SƠ ĐỀ XUẤT CẤP ĐỘ

6.1. Thẩm định tính hợp lệ của Hồ sơ

Tài liệu, nội dung HSĐXCĐ phải đáp ứng yêu cầu theo quy định tại Điều 15, Nghị định 85/2016/NĐ-CP. Đơn vị thẩm định (ĐVTĐ) kiểm tra xem HSĐXCĐ có tài liệu và thuyết minh đáp ứng yêu cầu sau hay không? Bao gồm:

6.1.1. Tài liệu thiết kế

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.

Lưu ý:

- Trường hợp đối với dự án đầu tư xây dựng mới hoặc mở rộng, nâng cấp hệ thống thông tin thì thuyết minh đề xuất cấp độ, lồng ghép vào nội dung của báo cáo nghiên cứu khả thi, dự án khả thi ứng dụng công nghệ thông tin hoặc báo cáo đầu tư của dự án, gửi cơ quan chức năng thẩm định, trình cơ quan có thẩm quyền phê duyệt báo cáo nghiên cứu khả thi; dự án khả thi ứng dụng công nghệ thông tin hoặc báo cáo đầu tư theo quy định của pháp luật về đầu tư.

- Trong trường hợp thuê dịch vụ công nghệ thông tin, đơn vị chủ trì thuê dịch vụ xây dựng thuyết minh đề xuất cấp độ, lồng ghép vào nội dung của kế hoạch, dự án thuê dịch vụ, gửi cơ quan chức năng thẩm định, trình cơ quan có thẩm quyền phê duyệt theo quy định của pháp luật về thuê dịch vụ công nghệ thông tin.

6.1.2. Thuyết minh HSĐXCĐ

1) Tài liệu thuyết minh Hồ sơ cấp độ, bao gồm các nội dung chính sau:

- Mô tả tổng quan về hệ thống thông tin

- Thuyết minh đề xuất cấp độ

- Thuyết minh phương án bảo đảm an toàn hệ thống thông tin theo cấp độ.

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

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

6.1.3. Các biểu mẫu hồ sơ kèm theo

Các biểu mẫu sử dụng trung quá trình thẩm định và phê duyệt HSĐXCĐ theo quy định bao gồm:

Mẫu số	Tên Văn bản	Biểu mẫu
01	Văn bản đề nghị thẩm định, phê duyệt hồ sơ đề xuất cấp độ	Mau01-ND85
02	Văn bản đề nghị thẩm định hồ sơ đề xuất cấp độ	Mau02-ND85
03	Văn bản xin ý kiến chuyên môn về hồ sơ đề xuất cấp độ	Mau03-ND85
04	Ý kiến thẩm định hồ sơ đề xuất cấp độ	Mau04-ND85
05	Tờ trình phê duyệt hồ sơ đề xuất cấp độ	Mau05-ND85
06	Quyết định phê duyệt cấp độ an toàn hệ thống thông tin	Mau06-ND85
07	Quyết định phê duyệt phương án bảo đảm an toàn thông tin	Mau07-ND85

6.2. Thẩm định sự phù hợp về việc đề xuất cấp độ

ĐVTĐ căn cứ vào nội dung thuyết minh mô tả, thuyết minh tổng quan về hệ thống thông tin để xác định phạm vi, quy mô của hệ thống.

Căn cứ vào nội dung thuyết minh về đề xuất cấp độ an toàn hệ thống thông tin trong HSĐXCĐ để xác định loại thông tin hệ thống đó xử lý theo quy định tại khoản 1, Điều 6 Nghị định 85/2016/NĐ-CP; Loại hình hệ thống thông tin đó theo quy định tại khoản 2, Điều 6, Nghị định 85/2016/NĐ-CP và Điều 4 Thông tư 03/2017/TT-BTTTT.

Căn cứ vào nội dung thuyết minh liên quan ở trên và căn cứ vào tiêu chí xác định cấp độ quy định tại Nghị định 85/2016/NĐ-CP từ Điều 7 đến Điều 11 để có căn cứ thẩm định xem cấp độ đề xuất có phù hợp hay không?

6.3. Thẩm định sự phù hợp của phương án bảo đảm an toàn thông tin

Tài liệu thiết kế là cơ sở để ĐVTĐ xem xét phương án bảo đảm an toàn thông tin được thuyết minh có phù hợp hay không? Tài liệu này mô tả chi tiết phương án thiết kế, lựa chọn các biện pháp bảo đảm an toàn thông tin cụ thể cũng như các thông tin khác liên quan đến hệ thống.

Do đó, ĐVTĐ kiểm tra xem trong tài liệu thiết kế có các nội dung sau hay không? Bao gồm:

1) Mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin.

2) Mô tả thiết kế và các thành phần của hệ thống thông tin.

3) Mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin.

4) Mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin.

Trường hợp, tài liệu thiết kế chưa có hoặc chưa đầy đủ những nội dung như ở trên, ĐVTĐ yêu cầu ĐVVH cung cấp, bổ sung.

Lưu ý: Trường hợp tài liệu thiết kế có nội dung không liên quan đến việc thuyết minh các phương án bảo đảm an toàn thông tin thì có thể lược bỏ để tinh gọn tài liệu.

6.4. Thẩm định sự phù hợp của phương án bảo đảm an toàn thông tin

Sự phù hợp của phương án bảo đảm an toàn thông tin là việc thuyết minh phương án trong HSĐXCĐ có đáp ứng các yêu cầu an toàn hay không? Lưu ý rằng, tại thời điểm thẩm định HSĐXCĐ mọi yêu cầu an toàn chưa phải đáp ứng hoàn toàn. Đối với các yêu cầu an toàn mà hệ thống chưa đáp ứng hoặc sẽ đáp ứng (đối với hệ thống xây dựng mới) phải chỉ ra phương án sẽ thực hiện để đáp ứng yêu cầu an toàn đó thế nào?

Đối với yêu cầu an toàn về quản lý, ĐVTĐ kiểm tra thuyết minh HSĐXCĐ đã có các chính sách, quy định (có thể được ban hành dưới dạng quy chế bảo đảm an toàn thông tin của cơ quan, tổ chức) đáp ứng yêu cầu an toàn về quản lý đặt ra hay chưa? Trường hợp đáp ứng yêu cầu, ĐVTĐ phải kiểm tra xem chính sách/quy định đó đã được ban hành ở văn bản nào? Trường hợp chưa đáp ứng, ĐVTĐ kiểm tra trong HSĐXCĐ có phương án/kế hoạch sửa đổi, bổ sung/thêm mới quy chế, chính sách an toàn thông tin nhằm đáp ứng yêu cầu đặt ra hay không?

Đối với yêu cầu an toàn về kỹ thuật, ĐVTĐ kiểm tra thuyết minh HSĐXCĐ đã mô tả việc thiết lập/phương án thiết kế, thiết lập, cấu hình hệ thống đáp ứng yêu cầu đặt ra hay chưa? Trường hợp đáp ứng yêu cầu, ĐVTĐ phải kiểm tra xem việc thiết kế, thiết lập, cấu hình đã được thực hiện như thế nào, trên thiết bị nào và đáp ứng các yêu cầu nào? Trường hợp chưa đáp ứng, ĐVTĐ kiểm tra trong HSĐXCĐ có phương án/kế hoạch nâng cấp, điều chỉnh hệ thống nhằm đáp ứng yêu cầu đặt ra hay không?

Việc thuyết minh phương án bảo đảm an toàn thông tin đáp ứng yêu cầu an toàn trong tiêu chuẩn quốc gia TCVN:11930 thì hoàn toàn đáp ứng các yêu cầu bắt buộc trong Thông tư 03/2017/TT-BTTTT. Do đó, ĐVTĐ thẩm định phương án bảo đảm an toàn thông tin trong HSĐXCĐ theo hướng dẫn trong chương 5.

Phương án bảo đảm an toàn thông tin được thuyết minh trong HSĐXCĐ phải thống nhất và phù hợp với thông tin liên quan trong tài liệu thiết kế.

Thuyết minh phương án bảo đảm an toàn thông tin được coi là đáp ứng yêu cầu khi đối với từng yêu cầu an toàn phải có thuyết minh tương ứng.

Chương VII
HƯỚNG DẪN BẢO VỆ HỆ THỐNG THÔNG TIN THEO CẤP ĐỘ

7.1. Tổ chức bảo đảm an toàn thông tin

Tổ chức bảo đảm an toàn thông tin và nhiệm vụ đầu tiên cơ quan, tổ chức cần thực hiện trong công tác bảo đảm an toàn hệ thống thông tin theo cấp độ.

Theo đó, người đứng đầu của cơ quan, tổ chức là chủ quản hệ thống thông tin có trách nhiệm: (1) Chỉ đạo và phụ trách công tác bảo đảm an toàn thông tin trong hoạt động của cơ quan, tổ chức mình; (2) Trong trường hợp chưa có đơn vị chuyên trách về an toàn thông tin độc lập: Chỉ định đơn vị chuyên trách về công nghệ thông tin làm nhiệm vụ đơn vị chuyên trách về an toàn thông tin và thành lập hoặc chỉ định bộ phận chuyên trách về an toàn thông tin trực thuộc đơn vị chuyên trách về công nghệ thông tin.

Đối với CQHTTT chỉ đạo ĐVVH thực hiện: (1) Lập HSĐXCĐ; tổ chức thẩm định, phê duyệt HSĐXCĐ; (2) Tổ chức thực hiện phương án bảo đảm an toàn hệ thống thông tin theo cấp độ theo phương án được phê duyệt trong HSĐXCĐ; (3) Triển khai công tác kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin; (4) Tổ chức thực hiện đào tạo ngắn hạn, tuyên truyền, phổ biến, nâng cao nhận thức và diễn tập về an toàn thông tin.

Đối với ĐVVH tổ chức thực hiện: (1) Thực hiện xác định cấp độ an toàn hệ thống thông tin theo chỉ đạo của CQHTTT; (2) Triển khai phương án bảo đảm an toàn hệ thống thông tin theo cấp độ theo phương án được phê duyệt trong HSĐXCĐ; (3) Tổ chức đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin theo quy định hoặc theo yêu cầu của cơ quan chức năng; (4) Báo cáo công tác thực thi bảo đảm an toàn hệ thống thông tin theo quy định hoặc theo yêu cầu của cơ quan chức năng; (5) Phối hợp, thực hiện theo yêu cầu của cơ quan chức năng liên quan của Bộ Thông tin và Truyền thông trong công tác bảo đảm an toàn thông tin.

7.2. Triển khai phương án bảo đảm an toàn hệ thống thông tin

Sau khi HSĐXCĐ được thẩm định và phê duyệt. ĐVVH căn cứ vào phương án đã được đề xuất để lên kế hoạch và tổ chức triển khai phương án bảo đảm an toàn thông tin đã được phê duyệt.

Đối với phương án về quản lý, ĐVVH dự thảo (bổ sung, sửa đổi, cập nhật) quy chế, chính sách bảo đảm an toàn thông tin theo phương án trong HSĐXCĐ và tham mưu cho CQHTTT ban hành.

Đối với phương án về kỹ thuật ngoài việc thiết lập cấu hình hệ thống thì còn liên quan đến đầu tư giải pháp kỹ thuật. Do đó, ĐVVH lên kế hoạch, phương án đầu tư, nâng cấp hệ thống để đáp ứng các yêu cầu kỹ thuật đặt ra.

Lưu ý: Đối với hệ thống thông tin cấp độ 3 trở xuống ưu tiên các phương án chia sẻ, dùng chung thiết bị/hạ tầng để giảm thiểu chi phí đầu tư.

7.3. Kiểm tra đánh giá và quản lý rủi ro an toàn thông tin

Yêu cầu an toàn đưa ra tại Thông tư 03/2017/TT-BTTTT và tiêu chuẩn quốc gia TCVN:11930 là các yêu cầu tối thiểu, cơ bản. Hệ thống thông tin đáp ứng các yêu câu này chỉ mới đáp ứng các yêu cầu cơ bản.

Trên thực tế, mỗi hệ thống thông tin khác nhau phải đối mặt với các nguy cơ mất an toàn thông tin khác nhau, tùy theo đặc trưng hay dịch vụ mà hệ thống đó cung cấp. Để thực hiện bảo vệ hệ thống thông tin một cách toàn diện, đầy đủ theo yêu cầu, đặc trưng riêng của từng hệ thống, một hệ thống thông tin sau khi đáp ứng các yêu cầu tối thiểu, cơ bản thì cần thực hiện đánh giá rủi ro để có phương án xử lý rủi ro và bổ sung thêm các biện pháp bảo đảm an toàn thông tin cần thiết.

Theo quy định tại Thông tư 03/2017/TT-BTTTT, hệ thống thông tin cấp độ 2 định kỳ 02 năm phải thực hiện kiểm tra, đánh giá rủi ro an toàn thông tin, hệ thống thông tin cấp độ 3 và 4 định kỳ 01 năm và hệ thống thông tin cấp độ 5 định kỳ 06 tháng.

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.

Cơ quan, tổ chức có thể tham khảo tiêu chuẩn quốc gia ISO/IEC 27005:2008 "Công nghệ thông tin- Kỹ thuật an toàn - Quản lý rủi ro an ninh thông tin" (Information technology - Security techniques - Information security risk management) để có thông tin tham khảo và phương án thực kiện kiểm tra, đánh giá và quản lý rủi ro cho hệ thống thông tin của mình.

7.4. Triển khai phương án giám sát an toàn thông tin

Để chủ động trong việc đối phó với những sự cố mất an toàn thông tin, ngoài việc thiết lập cấu hình hệ thống đáp ứng các yêu cầu kỹ thuật thì việc tổ chức triển khai phương án giám sát an toàn thông tin trong quá trình quản lý vận hành là rất quan trọng.

Về yêu cầu kỹ thuật, hệ thống thống thông tin cấp độ 3 trở lên phải có hệ thống giám sát tập trung bao gồm hai loại hình giám sát: (1) Giám sát hoạt động của hệ thống để có được thông tin trạng thái hoạt động của hệ thống về hiệu năng,

trạng thái tăng/giảm (Up/Down), băng thông kết nối; (2) Giám sát an toàn thông tin để phát hiện và cảnh báo sớm tấn công mạng và các nguy cơ mất an toàn thông tin.

Về yêu cầu quản lý đưa ra các quy định về: Quản lý vận hành hoạt động bình thường của hệ thống giám sát; Đối tượng giám sát bao gồm; Kết nối và gửi nhật ký hệ thống; Truy cập và quản trị hệ thống giám sát; Loại thông tin cần được giám sát; Lưu trữ và bảo vệ thông tin giám sát; Theo dõi, giám sát và cảnh báo sự cố; Bố trí nguồn lực và tổ chức giám sát.

Nội dung, phương thức, hệ thống kỹ thuật phục vụ công tác giám sát, cơ quan, tổ chức thực hiện theo quy định tại Điều 5 Thông tư số 31/2017/TT-BTTTT.

Chủ quản hệ thống thông tin có trách nhiệm chỉ đạo triển khai hoạt động giám sát đối với hệ thống thông tin thuộc phạm vi quản lý theo quy định tại Điều 14 Thông tư số 31/2017/TT-BTTTT.

7.5. Kiểm tra đánh giá an toàn thông tin

Việc kiểm tra đánh giá an toàn thông tin là hoạt động phải thực hiện thường xuyên để tăng cường khả năng phòng chống của hệ thống trước các nguy cơ mất an toàn thông tin từ các điểm yếu an toàn thông tin, lỗi thiết lập/cấu hình hệ thống và các nguy cơ mất an toàn thông tin khác. Nội dung, phương án kiểm tra đánh giá an toàn thông tin được quy định trong chương IV Thông tư 03/2017/TT-BTTTT. Trong đó, nội dung kiểm tra đánh giá bao gồm: (1) Kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ; (2) Đánh giá hiệu quả của biện pháp bảo đảm an toàn hệ thống thông tin;(3) Đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống.

Theo quy định ĐVVH phải thực hiện kiểm tra, đánh giá an toàn thông tin theo quy định và theo yêu cầu của cơ quan có thẩm quyền. Cấp có thẩm quyền yêu cầu kiểm tra, đánh giá là một trong các trường hợp sau: Bộ trưởng Bộ Thông tin và Truyền thông; Chủ quản hệ thống thông tin đối với hệ thống thông tin thuộc thẩm quyền quản lý; Đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin đối với hệ thống thông tin do đơn vị này phê duyệt hồ sơ đề xuất cấp độ.

Đơn vị được giao chủ trì nhiệm vụ kiểm tra, đánh giá là một trong những tổ chức sau đây: Cục An toàn thông tin; Đơn vị chuyên trách về an toàn thông tin; và các đơn vị khác có liên quan.

Thực hiện theo quy định, ĐVVH phải lập kế hoạch đánh giá định kỳ cho năm sau trình cấp có thẩm quyền phê duyệt để làm cơ sở triển khai thực hiện. Cụ thể:

- Thực hiện kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ theo quy định tại Điều 11 Thông tư 03/2017/TT-BTTTT.

- Thực hiện đánh giá hiệu quả của biện pháp bảo đảm an toàn thông tin tại Điều 12 Thông tư 03/2017/TT-BTTTT.

- Thực hiện đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống theo quy định tại Điều 13 Thông tư 03/2017/TT-BTTTT.

7.6. Xây dựng phương án ứng cứu sự cố an toàn thông tin mạng

Việc xây dựng phương án ứng cứu sự cố an toàn thông tin mạng giúp cơ quan, tổ chức chủ động hơn trong việc xử lý sự cố và khôi phục hệ thống sau sự cố.

Cơ quan, tổ chức phải xây dựng phương án quản lý sự cố an toàn thông tin đáp ứng yêu cầu an toàn về quản lý như trong tài liệu này, bao gồm các nội dung: Đưa ra chính sách/quy trình thực hiện quản lý sự cố an toàn thông tin của tổ chức, bao gồm: Phân nhóm sự cố an toàn thông tin; Phương án tiếp nhận, phát hiện, phân loại và xử lý thông tin; Kế hoạch ứng phó sự cố an toàn thông tin; Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin; Quy trình ứng cứu sự cố an toàn thông tin thông thường; Quy trình ứng cứu sự cố an toàn thông tin nghiêm trọng; Cơ chế phối hợp trong việc xử lý, khắc phục sự cố an toàn thông tin; Diễn tập phương án xử lý sự cố an toàn thông tin.

Thực hiện theo quy định tại Quyết định số 05/2017/NĐ-CP ngày 16/3/2017 quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia. Cụ thể, cơ quan, tổ chức phải thực hiện: Phân nhóm sự cố an toàn thông tin mạng; Xây dựng hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia; và thực hiện các trách nhiệm liên quan được quy định tại Quyết định này.

PHỤ LỤC I
HỒ SƠ ĐỀ XUẤT CẤP ĐỘ MẪU CHO TRUNG TÂM TÍCH HỢP DỮ LIỆU

ỦY BAN NHÂN DÂN TỈNH A
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

HỒ SƠ MẪU

HỒ SƠ ĐỀ XUẤT CẤP ĐỘ CHO TRUNG TÂM TÍCH HỢP DỮ LIỆU CỦA TỈNH A

Tỉnh A - 2019

THUẬT NGỮ, TỪ VIẾT TẮT

STT	Từ viết tắt	Nghĩa đầy đủ
1.	CNTT	Công nghệ thông tin
2.	CSDL	Cơ sở dữ liệu
3.	DVCTT	Dịch vụ công trực tuyến
4.	MCĐT	Một cửa điện tử
5.	WAN	Mạng tin học diện rộng
6.	LAN	Mạng nội bộ
7.	TSLCD	Mạng Truyền số liệu chuyên dùng
8.	VPN	Vitural Private Network
9.	DNS	Domain Name Server

PHẦN I. THÔNG TIN TỔNG QUAN VỀ HỆ THỐNG THÔNG TIN

1. Thông tin Chủ quản hệ thống thông tin

- Tên Tổ chức: UBND Tỉnh A.

- Quy định chức năng, nhiệm vụ và quyền hạn:

- Người đại diện: Ông Trần Văn A, Chức vụ: Chủ tịch UBND Tỉnh.

- Địa chỉ: địa chỉ trụ sở của đơn vị.

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

2. Thông tin Đơn vị vận hành

- Tên Đơn vị vận hành: Sở Thông tin và Truyền Thông tỉnh A.

- Quy định chức năng, nhiệm vụ và quyền hạn: Quyết định số …/QĐ-UBND ngày .../.../20xx

- Người đại diện: Ông Nguyễn Văn B, Chức vụ: Giám đốc.

- Địa chỉ: địa chỉ trụ sở của đơn vị.

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

3. Mô tả phạm vi, quy mô của hệ thống

- Phạm vi, quy mô của Hệ thống thông tin A: Hệ thống thông tin của tỉnh A được thiết lập để phục vụ công tác chỉ đạo điều hành và cung cấp dịch vụ công trực tuyến trong phạm vi tỉnh A. Quy mô của hệ thống cung cấp dịch vụ cho hơn 10.000 người sử dụng.

- Đối tượng phục vụ của hệ thống: Cơ quan, tổ chức, doanh nghiệp trên địa bản tỉnh A.

- Danh mục các hệ thống thông tin thành phần/các dịch vụ được cung cấp bởi trung tâm tích hợp dữ liệu:

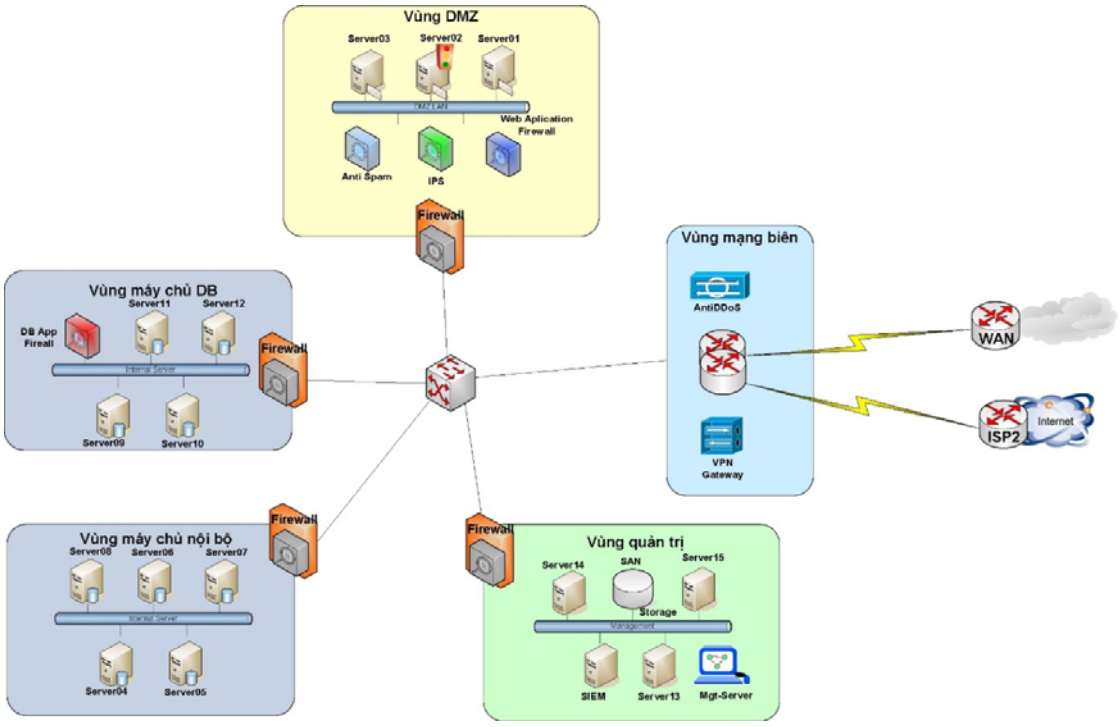
+ Hệ thống cổng thông tin nội bộ;

+ Hệ thống quản lý văn bản;

+ Hệ thống cung cấp dịch vụ công trực tuyến cấp độ 4.

4. Mô tả cấu trúc của hệ thống

4.1. Sơ đồ logic tổng thể



Hình 1. Cấu trúc logic của Trung tâm dữ liệu

Các vùng mạng được thiết kế như sau:

+ Vùng mạng biên được thiết kế để kết nối hệ thống mạng TTDL 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.

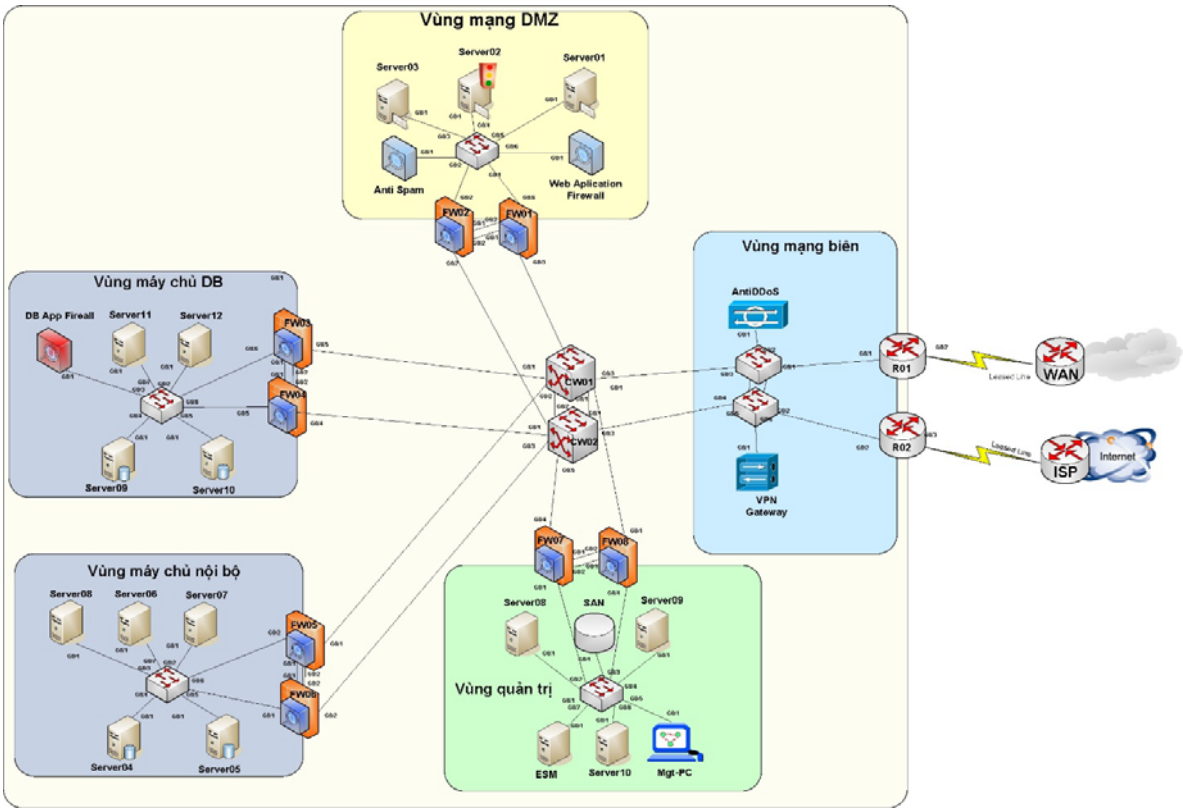
+ Vùng DMZ đặt các máy chủ công cộng, cung cấp dịch vụ ra bên ngoài Internet. Vùng mạng này triển khai thiết bị phòng chống xâm nhập IPS, thiết bị Web Application Firewall, thiết bị Anti-Spam.

+ 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.

+ Vùng máy chủ cơ sở dữ liệu đặt các máy chủ cơ sở dữ liệu phục vụ việc lưu trữ và quản lý cơ sở dữ liệu tập trung trên hệ thống. Vùng mạng này triển khai thiết bị phòng chống xâm nhập IPS, thiết bị DB Firewall CSDL.

4.2. Sơ đồ kết nối vật lý



Hình 2. Kết nối vật lý của Trung tâm dữ liệu

4.3. Danh mục thiết bị sử dụng trong hệ thống

Bảng 1. Danh mục thiết bị sử dụng trong hệ thống

STT	Tên thiết bị/ Chủng loại	Vị trí triển khai	Mục đích sử dụng
1	R01/Cisco3800	Vùng mạng biên	Kết nối và định tuyến động với các Router của 02 ISP.
2	R02/Cisco3800	Vùng mạng biên	Kết nối và định tuyến động với các Router của 02 ISP (Dự phòng nóng cho R01).
3	FW01/ASA5505	Vùng DMZ	Quản lý truy cập vào/ra và bảo vệ vùng mạng DMZ.
4	FW02/ASA5505	Vùng DMZ	Quản lý truy cập vào/ra và bảo vệ vùng mạng (Dự phòng nóng cho FW01).
5	FW03/Fortigate100C	Vùng máy chủ DB	Quản lý truy cập vào/ra và bảo vệ vùng máy chủ DB.

6	FW04/Fortigate100C	Vùng máy chủ DB	Quản lý truy cập vào/ra và bảo vệ vùng máy chủ DB (Dự phòng nóng cho FW03) …
7	…	…	….

4.4. Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống

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

STT	Tên dịch vụ	Máy chủ/Ứng dụng cài đăt/Vùng mạng/HĐH	Mục đích sử dụng
1	Cổng thông tin nội bộ	1) Server01/Cài đặt Web-App /Vùng DMZ/HĐH Centos7 2) Server11/Cài đặt BD/Vùng DB/HĐH Win2k8	Cung cấp thông tin công khai cho người sử nội bộ.
2	Quản lý văn bản	1) Server07/Cài đặt Web-App/Vùng máy chủ nội bộ/HĐH Centos7 2) Server12/Cài đặt BD/Vùng DB/HĐH Win2k8	Cung cấp ứng dụng quản lý văn bản cho cán bộ bên trong hệ thống.
3	Dịch vụ công trực tuyến	1) Server02/Cài đặt Reserver Proxy/Vùng DMZ/HĐH Centos7 2) Server06/Cài đặt Web-App/Vùng máy chủ nội bộ/HĐH Centos7 3) Server10/Cài đặt BD/Vùng DB/HĐH Centos	Cung cấp dịch vụ công trực tuyến cho người dân và doanh nghiệp
4	…	…	

4.5. Quy hoạch địa chỉ IP các vùng mạng trong hệ thống

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

STT	Vùng mạng	IP Private	IP Public
1	DMZ	192.168.1.0/24	202.191.x.0/24
2	Vùng mạng quản trị	192.168.2.0/24	202.191.y.0/24
3	Vùng máy chủ nội bộ	192.168.3.0/24	202.191.z.0/24
4	Vùng máy chủ DB	192.168.4.0/24	202.191.t.0/24

PHẦN II. THUYẾT MINH CẤP ĐỘ ĐỀ XUẤT

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

Hệ thống trung tâm tích hợp dữ liệu của tỉnh A bao gồm các hệ thống thành phần với cấp độ đề xuất tương ứng, bao gồm:

Bảng 4: Danh mục hệ thống thông tin và cấp độ đề xuất

STT	Hệ thống	Cấp độ đề xuất	Căn cứ đề xuất
1	Hệ thống cổng thông tin nội bộ	1	Khoản 1/Điều 7/NĐ85
2	Hệ thống quản lý văn bản	2	Khoản 1/Điều 8/NĐ85
3	Hệ thống cung cấp dịch vụ công trực tuyến cấp độ 4	3	Điểm a, khoản 2/Điều 9/NĐ85
4	…	…	…

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

2.1. Hệ thống mạng LAN nội bộ

Hệ thống cổng thông tin nội bộ chỉ xử lý thông tin công khai và phục vụ hoạt động nội bộ cho cán bộ của Sở TT&TT. Căn cứ theo quy định tại Khoản 1/Điều 7/NĐ85, hệ thống này được đề xuất cấp độ 1.

2.2. Hệ thống một cửa điện tử

Hệ thống quản lý văn bản có xử lý thông tin riêng của Sở TT&TT và phục vụ hoạt động nội bộ cho cán bộ của Sở TT&TT. Căn cứ theo quy định tại Khoản 1/Điều 8/NĐ85, hệ thống này được đề xuất cấp độ 2.

2.3. Hệ thống cung cấp dịch vụ công trực tuyến cấp độ 4

Hệ thống cung cấp dịch vụ công trực tuyến cấp độ 4 cung cấp dịch vụ trực tuyến cho người dân, doanh nghiệp với quy mô cung cấp dịch vụ cho hơn 10.000 sử dụng. Căn cứ theo quy định tại điểm a hoặc c, khoản 2/Điều 9/NĐ85, hệ thống được đề xuất cấp độ 3.

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

Thuyết minh phương án về quản lý bao gồm các nội dung sau:

1. Thiết lập chính sách an toàn thông tin.

2. Tổ chức bảo đảm an toàn thông tin.

3. Bảo đảm nguồn nhân lực.

4. Quản lý thiết kế, xây dựng hệ thống.

5. Quản lý vận hành hệ thống.

- Quản lý an toàn mạng;
- Quản lý an toàn máy chủ và ứng dụng;
- Quản lý an toàn dữ liệu;
- 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;
- Quản lý sự cố an toàn thông tin;
- Quản lý an toàn người sử dụng đầu cuối.

Đối với những yêu cầu quản lý chưa đáp ứng các yêu cầu an toàn trong Thuyết minh này, Đơn vị vận hành sẽ cập nhật, bổ sung trình Chủ quản hệ thống thông tin ban hành trong vòng 06 tháng, kể từ khi HSĐXCĐ được phê duyệt.

Thuyết minh phương án về kỹ thuật bao gồm các nội dung:

1. Bảo đảm an toàn mạng.

1.1. Thiết kế hệ thống;

1.2. Kiểm soát truy cập từ bên ngoài mạng;

1.3. Kiểm soát truy cập từ bên trong mạng;

1.4. Nhật ký hệ thống;

1.5. Phòng chống xâm nhập;

1.6. Phòng chống phần mềm độc hại trên môi trường mạng;

1.7. Bảo vệ thiết bị hệ thống.

2. Bảo đảm an toàn máy chủ.

2.1. Xác thực;

2.2. Kiểm soát truy cập;

2.3. Nhật ký hệ thống;

2.4. Phòng chống xâm nhập;

2.5. Phòng chống phần mềm độc hại;

2.6. Xử lý máy chủ khi chuyển giao.

3. Bảo đảm an toàn ứng dụng.

3.1. Xác thực;

3.2. Kiểm soát truy cập;

3.3. Nhật ký hệ thống;

3.4. Bảo mật thông tin liên lạc;

3.5. Chống chối bỏ.

4. Bảo đảm an toàn dữ liệu.

4.1. Nguyên vẹn dữ liệu;

4.2. Bảo mật dữ liệu;

4.3. Sao lưu dự phòng.

Đối với các yêu cầu kỹ thuật chưa đáp ứng yêu cầu an toàn cơ bản trong Thuyết minh này, Đơn vị vận hành sẽ triển khai nâng cấp, thiết lập cấu hình hệ thống để đáp ứng yêu cầu trong vòng 18 tháng, kể từ khi HSĐXCĐ được phê duyệt.

Căn cứ vào nội dung thuyết minh đề xuất cấp độ ở Mục II, phần 1. Trung tâm tích hợp dữ liệu của tỉnh A bao gồm nhiều hệ thống thành phần khác nhau. Mỗi hệ thống thành phần được đề xuất cấp độ khác nhau. Đối với từng hệ thống thành phần khác nhau thì có phương án bảo đảm an toàn thông tin khác nhau để đáp ứng các yêu cầu an toàn với cấp độ tương ứng.

Thuyết minh phương án bảo đảm an toàn thông tin về quản lý đưa ra các quy định liên quan đến con người và quy trình. Các yêu cầu quản lý ở cấp độ cao hơn khi được đáp ứng thì cũng đáp ứng các yêu cầu ở cấp độ thấp hơn. Do đó, thuyết minh phương án bảo đảm an toàn thông tin về quản lý được thuyết minh chung tại Phụ lục I.

Thuyết minh phương án bảo đảm an toàn thông tin về kỹ thuật liên quan đến việc thiết kế, thiết lập cấu hình hệ thống và liên quan trực tiếp đến đầu tư. Do đó,

thuyết minh phương án về kỹ thuật được thuyết minh theo từng hệ thống thành phần theo cấp độ tương ứng theo nguyên tắc sau:

Đối với hạ tầng, thiết bị hệ thống, máy chủ dùng chung để bảo vệ nhiều hệ thống thành phần khác nhau, thì hạ tầng, thiết bị hệ thống, máy chủ đó phải được thiết kế, thiết lập để đáp ứng yêu cầu của hệ thống thành phần có cấp độ cao nhất.

Đối với hạ tầng, thiết bị hệ thống, máy chủ dùng riêng, độc lập đối với từng hệ thống thành phần, thì hạ tầng, thiết bị hệ thống, máy chủ đó phải được thiết kế, thiết lập để đáp ứng yêu cầu của hệ thống thành phần với cấp độ tương ứng nhằm bảo đảm tiết kiệm và hiệu quả.

Trên cơ sở đó, thuyết minh phương án bảo đảm an toàn thông tin cho trung tâm tích hợp dữ liệu của tỉnh A sẽ bao gồm các thuyết minh thành phần sau:

Bảng 5: Các thuyết minh thành phần

STT	Hệ thống	Cấp độ đề xuất	Nội dung thuyết minh
1	Thuyết minh phương án bảo đảm an toàn thông tin về quản lý	3	Phụ lục I
2	Thuyết minh phương án kỹ thuật đối với hệ thống cổng thông tin nội bộ	1	Phụ lục II
3	Thuyết minh phương án kỹ thuật đối với hệ thống quản lý văn bản	2	Phụ lục III
4	Thuyết minh phương án kỹ thuật đối với hệ thống cung cấp dịch vụ công trực tuyến	3	Phụ lục IV

PHỤ LỤC I. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM AN TOÀN THÔNG TIN VỀ QUẢN LÝ VỚI CẤP ĐỘ 3

1. Thiết lập chính sách an toàn thông tin

1.1. Chính sách an toàn thông tin

Yêu cầu	Xác định các mục tiêu, nguyên tắc bảo đảm an toàn thông tin.
Phương án	1. Mục tiêu: Bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin. 2. Nguyên tắc bảo đảm an toàn thông tin: a) Hoạt động an toàn thông tin mạng của cơ quan, tổ chức, cá nhân phải đúng quy định của pháp luật, bảo đảm quốc phòng, an ninh quốc gia, bí mật nhà nước, giữ vững ổn định chính trị, trật tự, an toàn xã hội và thúc đẩy phát triển kinh tế - xã hội. b) Tổ chức, cá nhân không được xâm phạm an toàn thông tin mạng của tổ chức, cá nhân khác. c) Việc xử lý sự cố an toàn thông tin mạng phải bảo đảm quyền và lợi ích hợp pháp của tổ chức, cá nhân, không xâm phạm đến đời sống riêng tư, bí mật cá nhân, bí mật gia đình của cá nhân, thông tin riêng của tổ chức. d) Hoạt động an toàn thông tin mạng phải được thực hiện thường xuyên, liên tục, kịp thời và hiệu quả…
Yêu cầu	Xác định trách nhiệm của đơn vị chuyên trách về an toàn thông tin, các cán bộ làm về an toàn thông tin và các đối tượng thuộc phạm vi điều chỉnh của chính sách an toàn thông tin.
Phương án	Quy định trách nhiệm của cơ quan, tổ chức trên địa bàn trong công tác bảo đảm an toàn thông tin: 1. UBND tỉnh A có trách nhiệm thực hiện các nhiệm vụ của chủ quản hệ thống thông tin đối với các hệ thống thông tin trên địa bàn theo quy định tại Điều 20, Nghị định 85/2016/NĐ-CP. 2. Trách nhiệm của Sở Thông tin và Truyền thông a) Tham mưu Ủy ban nhân dân tỉnh và Ban chỉ đạo công tác bảo đảm an toàn thông tin mạng trên địa bàn tỉnh.

	b) Thực hiện trách nhiệm của đơn vị chuyên trách về an toàn thông tin theo quy định của pháp luật theo quy định tại Điều 21, Nghị định 85/2016/NĐ-CP. c) Thực hiện trách nhiệm của đơn vị vận hành đối với các hệ thống thông tin thuộc phạm vi quản lý. d) Làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng trên địa bàn tỉnh. e) Chủ trì, phối hợp với Văn phòng Ủy ban nhân dân tỉnh, Công an tỉnh và các đơn vị có liên quan tiến hành kiểm tra công tác bảo đảm an toàn thông tin mạng định kỳ hàng năm hoặc theo chỉ đạo của UBND tỉnh đối với các cơ quan nhà nước trong tỉnh. g) Tùy theo mức độ sự cố, phối hợp Cục An toàn thông tin hoặc Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam và các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố an toàn thông tin mạng. h) Tổng hợp và báo cáo về tình hình an toàn thông tin mạng theo định kỳ cho Bộ Thông tin và Truyền thông, Ủy ban nhân dân tỉnh theo quy định của pháp luật. i) Hàng năm, xây dựng và triển khai các chương trình đào tạo, tập huấn về công tác bảo đảm an toàn thông tin mạng cho cán bộ, công chức phụ trách an toàn thông tin mạng của các cơ quan, đơn vị. Tổ chức các hội nghị, hội thảo chuyên đề và tuyên truyền về an toàn thông tin mạng trong công tác quản lý nhà nước trên địa bàn tỉnh. k) Tổ chức tuyên truyền, hướng dẫn về công tác bảo đảm an toàn thông tin mạng. l) Phối hợp với Ban Tuyên giáo Tỉnh ủy, Công an tỉnh có các biện pháp phòng, chống các thông tin vi phạm pháp luật, ảnh hưởng đến an ninh quốc gia, trật tự, an toàn xã hội trên môi trường mạng, nhất là trên các cổng/trang thông tin điện tử, mạng xã hội. 3. Trách nhiệm của các cơ quan, đơn vị a) Thủ trưởng các cơ quan, đơn vị có trách nhiệm tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trong công tác bảo đảm an toàn thông tin mạng của cơ quan, đơn vị mình. b) Thực hiện trách nhiệm của đơn vị vận hành theo quy định tại Điều 22, Nghị định 85/2016/NĐ-CP.

	c) Phân công một bộ phận hoặc cán bộ phụ trách bảo đảm an toàn thông tin mạng của đơn vị, tạo điều kiện để các cán bộ được học tập, nâng cao trình độ về an toàn thông tin mạng. d) Bố trí, tạo điều kiện làm việc cho cán bộ chuyên trách về công nghệ thông tin trong các cơ quan, đơn vị phù hợp với chuyên môn, được ưu tiên bồi dưỡng nghiệp vụ về an toàn thông tin mạng. e) Xây dựng quy chế, quy trình về bảo đảm an toàn thông tin mạng phù hợp với Quy chế này và các quy định của pháp luật. g) Phối hợp, cung cấp thông tin và tạo điều kiện cho các đơn vị có thẩm quyền triển khai công tác kiểm tra khắc phục sự cố xảy ra một cách kịp thời, nhanh chóng và đạt hiệu quả. h) Phối hợp chặt chẽ với Sở Thông tin và Truyền thông, Công an tỉnh trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin mạng. i) Khuyến khích các cơ quan, đơn vị liên kết các tổ chức, cá nhân, doanh nghiệp CNTT mở các khóa đào tạo nhân lực trong lĩnh vực an toàn thông tin mạng. k) Hàng năm bố trí kinh phí cho việc ứng dụng công nghệ thông tin nói chung và công tác bảo đảm an toàn thông tin mạng nói riêng trong nội bộ cơ quan, đơn vị mình; lập kế hoạch nâng cấp, bảo trì, sửa chữa, gia hạn bản quyền phần mềm... cho các hệ thống phần cứng, phần mềm nhằm thực hiện tốt công tác bảo mật, bảo đảm an toàn thông tin mạng đưa vào dự toán chi năm sau để triển khai thực hiện. 4. Trách nhiệm của cán bộ, công chức, viên chức và người lao động trong các cơ quan, đơn vị a) Trách nhiệm của bộ phận chuyên trách về an toàn thông tin: i) Chịu trách nhiệm bảo đảm an toàn thông tin mạng của cơ quan, đơn vị; ii) Tham mưu lãnh đạo cơ quan ban hành các quy chế, quy trình nội bộ, triển khai các giải pháp kỹ thuật bảo đảm an toàn thông tin mạng; iii) Thực hiện việc giám sát, đánh giá, báo cáo Thủ trưởng cơ quan, đơn vị các rủi ro mất an toàn thông tin mạng và mức độ nghiêm trọng của các rủi ro đó;

	iv) Phối hợp với các cá nhân, đơn vị có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn thông tin mạng; v) Thường xuyên cập nhật nâng cao kiến thức, trình độ chuyên môn đáp ứng yêu cầu bảo đảm an toàn thông tin mạng của đơn vị. b) Trách nhiệm của người sử dụng: i) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao; ii) Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng; iii) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách công nghệ thông tin của cơ quan, đơn vị để kịp thời ngăn chặn và xử lý; iv) Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng được tỉnh hoặc đơn vị chuyên môn tổ chức.

1.2. Xây dựng và công bố

Yêu cầu	Quy định về xây dựng và công bố Quy chế bảo đảm an toàn thông tin.
Phương án	Xây dựng và công bố Quy chế bảo đảm an toàn thông tin: 1. Quy chế được lấy ý kiến cấp có thẩm quyền, đơn vị liên quan trước khi công bố áp dụng. 2. Quy chế được Sở TT&TT xây dựng trình Chủ tịch UBND tỉnh A ban hành.

1.3. Rà soát, sửa đổi

Yêu cầu	Có quy định về việc rà soát, sửa đổi Quy chế bảo đảm an toàn thông tin.
Phương án	Rà soát, sửa đổi Quy chế bảo đảm an toàn thông tin: 1. Định kỳ 02 năm hoặc khi có thay đổi Quy chế bảo đảm an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung. 2. Trong quá trình thực hiện Quy chế, nếu có vấn đề vướng mắc, phát sinh, các đơn vị phản ánh kịp thời về Sở Thông tin và Truyền thông để tổng hợp báo cáo Uỷ ban nhân dân tỉnh điều chỉnh, bổ sung.

2. Tổ chức bảo đảm an toàn thông tin

2.1. Đơn vị chuyên trách về an toàn thông tin

Yêu cầu	Thành lập hoặc chỉ định đơn vị/bộ phận chuyên trách về an toàn thông tin trong tổ chức.
Phương án	UBND tỉnh ban hành Quyết định giao Sở TT&TT là đơn vị chuyên trách về an toàn thông tin, trình Chủ tịch UBND tỉnh A ban hành. Phòng CNTT hoặc bộ phận chuyên trách CNTT dự thảo Quyết định trình giảm đốc Sở TT&TT là giao nhiệm vụ là bộ phận chuyên trách về an toàn thông tin.

2.2. Phối hợp với những cơ quan/tổ chức có thẩm quyền

Yêu cầu	Có quy định về việc phối hợp với những cơ quan/tổ chức có thẩm quyền.
Phương án	Phối hợp với những cơ quan/tổ chức có thẩm quyền: 1. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin: a) UBND tỉnh A giao Sở TT&TT là đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin tại Quyết định số 468/QĐ-UBND ngày 12/7/2016. b) Sở TT&TT làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng trên địa bàn tỉnh. c) Sở TT&TT chủ trì, phối hợp với Văn phòng Ủy ban nhân dân tỉnh, Công an tỉnh và các đơn vị có liên quan tiến hành kiểm tra công tác bảo đảm an toàn thông tin mạng định kỳ hàng năm hoặc theo chỉ đạo của UBND tỉnh đối với các cơ quan nhà nước trong tỉnh. 2. Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin: Tùy theo mức độ sự cố, phối hợp Cục An toàn thông tin hoặc Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam và các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố an toàn thông tin mạng

3. Tổ chức bảo đảm an toàn thông tin

3.1. Tuyển dụng

Yêu cầu	Có quy định về tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ.
Phương án	Quy định về tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ:

	1. Quy định cán bộ được tuyển dụng vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng. 2. Xây dựng quy trình tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ.

3.2. Trong quá trình làm việc

Yêu cầu	Có quy định về việc thực hiện bảo đảm an toàn thông tin trong quá trình làm việc.
Phương án	Quy định về việc thực hiện bảo đảm an toàn thông tin trong quá trình làm việc: 1. Trách nhiệm bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống a) Với người sử dụng: - Người sử dụng có trách nhiệm đảm bảo ATTT đối với từng vị trí công việc. Trước khi tham gia vào hệ thống phải được kiểm tra khả năng đáp ứng các yêu cầu về ATTT. - Phải được thường xuyên tổ chức quán triệt các quy định về ATTT, nhằm nâng cao nhận thức về trách nhiệm đảm bảo ATTT. - Cá nhân, tổ chức phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp thiết bị. b) Với cán bộ quản lý và vận hành hệ thống - Cán bộ chuyên trách phải thiết lập phương pháp hạn chế truy cập mạng không dây, giám sát và điều khiển truy cập không dây, tổ chức sử dụng chứng thực và mã hóa để bảo vệ truy cập không dây tới hệ thống thông tin. - Cán bộ chuyên trách phải tổ chức quản lý định danh đối với tất cả người dùng tham gia sử dụng hệ thống thông tin. 2. Định kỳ hàng năm người sử dụng được tổ chức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin theo chương trình, nội dung tại Quyết định số 893/QĐ-TTg ngày 19/6/2015 về việc phê duyệt Đề án Tuyên truyền, phổ biến, nâng cao nhận thức và trách nhiệm về an toàn thông tin đến năm 2020. 3. Định kỳ hàng năm người sử dụng được tổ chức đào tạo các kỹ năng

	cơ bản về an toàn thông tin theo chương trình, nội dung tại - Quyết định số 99/QĐ-TTg ngày 14/01/2014 phê duyệt Đề án Đào tạo và phát triển nguồn nhân lực an toàn, an ninh thông tin đến năm 2020.

3.3. Chấm dứt hoặc thay đổi công việc

Yêu cầu	Có quy định đối với cán bộ nghỉ hoặc thay đổi công việc.
Phương án	Quy định đối với cán bộ nghỉ hoặc thay đổi công việc: 1. Cán bộ nghỉ hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác thuộc sở hữu của tổ chứ. 2. Cán bộ quản trị phải vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc. 3. Cán bộ nghỉ hoặc thay đổi công việc phải có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc.

4. Quản lý thiết kế, xây dựng hệ thống thông tin

4.1. Thiết kế an toàn hệ thống thông tin

Yêu cầu	Có quy định về thiết kế an toàn hệ thống thông tin.
Phương án	Quy định đối với tài liệu thiết kế hệ thống: 1. Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin. 2. Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin. 3. Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin. 4. Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin. 5. Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống.

4.2. Phát triển phần mềm thuê khoán

Yêu cầu	Có quy định về phát triển phần mềm thuê khoán.
Phương án	Quy định đối với việc phát triển phần mềm thuê khoán: 1. Có điều khoản hợp đồng và các cam kết đối với bên thuê khoán khi thực hiện các nội dung liên quan đến việc phát triển phần mềm

	thuê khoán. 2. Các nhà phát triển cung cấp mã nguồn phần mềm. 3. Phần mềm thuê khoán phải được kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng. 4. Phần mềm thuê khoán phải được kiểm tra, đánh giá an toàn thông tin, trước khi đưa vào sử dụng.

4.3. Thử nghiệm và nghiệm thu hệ thống

Yêu cầu	Có quy định về việc thử nghiệm và nghiệm thu hệ thống.
Phương án	Quy định đối với việc thử nghiệm và nghiệm thu hệ thống: 1. Bên triển khai xây dựng kế hoạch, nội dung thử nghiệm hệ thống, trình cấp có thẩm quyền phê duyệt, trước khi thực hiện thử nghiệm và nghiệm thu hệ thống. 2. Hệ thống phải được thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng theo nội dung, kế hoạch được phê duyệt. 3. Có bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống. 4. Có đơn vị độc lập (bên thứ ba hoặc bộ phận độc lập thuộc đơn vị thực hiện tư vấn và giám sát quá trình thử nghiệm và nghiệm thu hệ thống 5. Có báo cáo nghiệm thu được xác nhận của bộ phận chuyên trách và phê duyệt của chủ quản hệ thống thông tin trước khi đưa vào sử dụng.

5. Quản lý vận hành hệ thống thông tin

5.1. Quản lý an toàn mạng

Yêu cầu	Có quy định về quản lý an toàn mạng.
Phương án	Quy định về quản lý an toàn mạng: 1. Hệ thống mạng phải được thiết kế thống nhất, cùng kết hợp và hỗ trợ, tương tác hoạt động với nhau, được tổ chức quản lý định danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý hệ thống chặt chẽ, bảo đảm an toàn và bảo mật. 2. Hệ thống mạng phải được thiết lập cấu hình để: Kiểm soát truy cập từ bên ngoài mạng; Kiểm soát truy cập từ bên trong mạng; Kết

	nối về hệ thống giám sát tập trung; Phòng chống xâm nhập giữa các vùng mạng; Phòng chống phần mềm độc hại trên môi trường mạng. 3. Các thiết bị mạng phải được cấu hình chức năng xác thực; Chỉ cho phép sử dụng các kết nối mạng an toàn (nếu hỗ trợ) khi truy cập, quản trị thiết bị từ xa; Giới hạn các địa chỉ mạng có thể kết nối, quản trị thiết bị từ xa; Hạn chế được số lần đăng nhập sai; Phân quyền truy cập, quản trị; Nâng cấp, xử lý điểm yếu an toàn thông tin của thiết bị hệ thống trước khi đưa vào sử dụng. 4. Hệ thống mạng phải được trang bị hệ thống kỹ thuật, công nghệ hiện đại để thường xuyên, liên tục quản lý, giám sát, kiểm soát mạng nhằm phát hiện, ngăn chặn các truy cập trái phép của người sử dụng, tin tặc tấn công; triển khai cơ chế phòng chống vi rút tin học, thư rác cho những hệ thống xung yếu (máy chủ thư điện tử, máy chủ website, máy chủ tên miền, v.v...) và tại các máy chủ, máy trạm khác trong hệ thống. 5. Việc thanh lý, tiêu hủy thiết bị, vật mang thông tin trong mạng Bộ phải đảm bảo yêu cầu không để lộ, lọt thông tin Nhà nước. Phải có quy trình cụ thể và phải lưu giữ hồ sơ, biên bản việc thanh lý, tiêu hủy. 6. Các yêu cầu đối với phòng máy chủ: a) Phòng máy chủ của các cơ quan là khu vực hạn chế tiếp cận và được được lắp đặt hệ thống camera giám sát. Chỉ những người có trách nhiệm theo quy định của Thủ trưởng cơ quan mới được phép vào phòng máy chủ. b) Phòng máy chủ phải có hệ thống lưu điện đủ công suất và duy trì thời gian hoạt động của các máy chủ tối thiểu 15 phút khi có sự cố mất điện. c) Bố trí cán bộ có năng lực chuyên môn cao để quản lý, vận hành phòng máy chủ và duy trì chế độ trực để đảm bảo an toàn thông tin mạng. 7. Đối với các thiết bị mạng chính a) Phải lắp đặt thiết bị chống sét để bảo vệ hệ thống CNTT, phải xây dựng ít nhất 02 thiết bị chống sét: một cho một đường cung cấp điện và một đường của mạng nội bộ (LAN). c) Thiết bị chuyển mạch (switch): Thiết bị chuyển mạch mạng tin

	học của các cơ quan phải đảm bảo khả năng cung cấp các chức năng quản trị nhằm tăng cường độ an toàn và bảo mật cho hệ thống mạng như: cung cấp khả năng từ chối các kết nối không mong muốn vào hệ thống trên từng cổng, quy định địa chỉ IP cho từng cổng và khống chế số lượng kết nối vào hệ thống mạng nội bộ thông qua thiết bị chuyển mạch. Phải có ít nhất 01 thiết bị chuyển mạch có hỗ trợ định tuyến IP (IP routing) cho mỗi mạng nội bộ, hỗ trợ chức năng điều khiển truy cập (Access Control List), hỗ trợ chức năng xác thực thiết bị và người sử dụng (User & Device Authentication) và chức năng bảo mật quản trị mạng (Network Administration Security). c) Tường lửa (firewall): Các cơ quan phải xây dựng tường lửa đảm bảo các yêu cầu gồm khả năng xử lý được số lượng kết nối đồng thời cao, hỗ trợ các công nghệ mạng riêng ảo thông dụng và có phần cứng mã hóa tích hợp để tăng tốc độ mã hóa dữ liệu, cung cấp đầy đủ các cơ chế bảo mật cơ bản như NAT, PAT, quản lý luồng dữ liệu vào, ra và có khả năng bảo vệ hệ thống trước các loại tấn công từ chối dịch vụ (DDoS). 8. Tệp tin cấu hình, sơ đồ mạng logic và vật lý phải được cập nhật, sao lưu dự phòng. 9. Có biện pháp bảo vệ, dự phòng, phòng chống các nguy cơ do mất cắp, cháy nổ, ngập lụt, động đất và các thảm họa khác do thiên nhiên hoặc con người gây ra và các phương án khôi phục hệ thống sau thảm họa.

5.2. Quản lý an toàn máy chủ và ứng dụng

Yêu cầu	Có quy định về quản lý an toàn máy chủ và ứng dụng.
Phương án	Quy định về quản lý an toàn máy chủ và ứng dụng: 1. Quy định với máy chủ a) Hệ thống máy chủ phải có tính năng sẵn sàng cao, cơ chế dự phòng linh hoạt để đảm bảo hoạt động liên tục. b) Có biện pháp bảo vệ, dự phòng, phòng chống các nguy cơ do mất cắp, cháy nổ, ngập lụt, động đất và các thảm họa khác do thiên nhiên hoặc con người gây ra và các phương án khôi phục sau thảm họa cho hệ thống máy chủ. c) Máy chủ phải được thiết lập chính sách xác thực; Kiểm soát truy cập; Kết nối về hệ thống giám sát tập trung; Thực hiện biện pháp

	phòng chống xâm nhập; Phòng chống phần mềm độc hại và xử lý dữ liệu trên máy chủ khi chuyển giao. d) Máy chủ phải được nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng. e) Việc kết nối, gỡ bỏ máy chủ khỏi hệ thống phải được sự cho phép của Thủ trưởng đơn vị và thực hiện theo quy trình đã được phê duyệt. g) Phần mềm hệ điều hành cài lên máy chủ ưu tiên là phần mềm hệ điều hành có bản quyền hoặc là phần mềm mã nguồn mở được sử dụng rộng rãi trong nước và quốc tế. h) Có tài liệu liệt kê, cài đặt với những phần mềm hệ thống cài trong máy chủ. 2. Quy định với ứng dụng: a) Các yêu cầu, thiết kế về an toàn bảo mật của phần mềm ứng dụng cần được xác định rõ trong tài liệu phân tích, thiết kế. Trong quá trình triển khai, vận hành các phần mềm ứng dụng cần đảm bảo nghiêm ngặt theo các yêu cầu, thiết kế về an toàn bảo mật. b) Ứng dụng phải được thiết lập chính sách xác thực; Kiểm soát truy cập; Kết nối về hệ thống giám sát tập trung; Có phương án bảo mật thông tin liên lạc, chống chối bỏ và biện pháp bảo đảm an toàn ứng dụng và mã nguồn. c) Có phương án xác định và khắc phục rủi ro trước, trong quá trình triển khai và khi vận hành các phần mềm ứng dụng. d) Ứng dụng phải kiểm tra, thử nghiệm và có biên bản đánh giá tính an toàn, bảo mật đối với phần mềm ứng dụng theo yêu cầu khi nghiệm thu các phần mềm này. Việc tiến hành thử nghiệm phải đảm bảo trên môi trường riêng biệt, không ảnh hưởng tới hoạt động và dữ liệu của đơn vị. 3. Quy định với ứng dụng thư điện tử: a) Không sử dụng các hộp thư điện tử công cộng. Không sử dụng thư điện tử chính thức của đơn vị vào mục đích cá nhân. b) Mỗi cá nhân cần đặt mật khẩu đủ mạnh cho hộp thư điện tử của mình. c) Đơn vị quản lý hệ thống thư điện tử cần có quy định về việc khóa và xóa bỏ hộp thư điện tử cá nhân khi cá nhân đó không còn làm

	việc tại đơn vị. d) Đơn vị quản lý hệ thống thư điện tử cần xây dựng phương án đảm bảo an toàn và tính khả dụng truy cập cho hệ thống thư điện tử trong nội bộ và trên Internet, phương án chống thư rác cho thư điện tử. e) Bảo đảm an toàn cho hệ thống thư điện tử: Thực hiện theo hướng dẫn tại công văn số 430/BTTTT-CATTT ngày 09 tháng 2 năm 2015 của Bộ TT&TT về việc hướng dẫn đảm bảo an toàn thông tin cho hệ thống thư điện tử của cơ quan, tổ chức nhà nước. 4. Quy định đối với cổng/trang thông tin điện tử a) Quản lý toàn bộ các phiên bản của mã nguồn, phối hợp với đơn vị thực hiện dịch vụ hosting tổ chức mô hình trang web hợp lý, tránh khả năng tấn công leo thang đặc quyền. Yêu cầu đơn vị cung cấp dịch vụ hosting phải cài đặt các hệ thống phòng vệ như tường lửa thiết bị phát hiện/phòng chống xâm nhập (IDS/IPS) ở mức ứng dụng web (WAF- Web Application Firewall). b) Các trang web khi đưa vào sử dụng hoặc khi bổ sung thêm các chức năng, dịch vụ công mới cần đánh giá kiểm định nhằm tránh được các lỗi bảo mật thường xảy ra trên ứng dụng web như: SQL Injection, Cross-Site Scripting (xss), ... c) Phối hợp với các nhà cung cấp dịch vụ hosting xây dựng phương án phục hồi trang web, trong đó chú ý mỗi tháng thực hiện việc backup toàn bộ nội dung trang web một lần bao gồm mã nguồn, cơ sở dữ liệu, dữ liệu phi cấu trúc, ... để bảo đảm khi có sự cố có thể khắc phục lại ngay trong vòng 24 giờ. d) Bảo đảm an toàn cho Cổng/Trang thông tin điện tử: Thực hiện theo hướng dẫn tại công văn số 2132/BTTTT-VNCERT ngày 18 tháng 7 năm 2011 của Bộ TT&TT về việc hướng dẫn đảm bảo an toàn thông tin cho các Cổng/Trang thông tin điện tử.

5.3. Quản lý an toàn dữ liệu

Yêu cầu	Có quy định về quản lý an toàn dữ liệu.
Phương án	Quy định về quản lý an toàn dữ liệu: 1. Thực hiện quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã kiểm tra tính nguyên vẹn. 2. Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện

	quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ. 3. Lưu trữ có mã hóa các thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trên hệ thống lưu trữ/phương tiện lưu trữ.

5.4. Quản lý an toàn thiết bị đầu cuối

Yêu cầu	Có quy định về quản lý thiết bị đầu cuối.
Phương án	Các thiết bị đầu cuối khi kết nối và hệ thống phải được quản lý như sau: 1. Thông tin về thiết bị đầu cuối (tên, chủng loại, địa chỉ MAC, địa chỉ IP) phải được quản lý và cập nhật. 2. Các thiết bị đầu cuối phải được quản lý khi kết nối vào hệ thống mạng theo địa chỉ MAC, IP. 3. Khi truy cập và sử dụng thiết bị đầu cuối từ xa phải có cơ chế xác thực và sử dụng giao thức mạng an toàn. 4. Việc cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống phải được cho phép bởi người có thẩm quyền và thực hiện theo quy trình được phê duyệt.

5.5. Quản lý phòng chống phần mềm độc hại

Yêu cầu	Có quy định về quản lý phòng chống phần mềm độc hại
Phương án	Quy định về quản lý phòng chống phần mềm độc hại: 1. Tất cả các máy trạm, máy chủ phải được trang bị phần mềm phòng chống mã độc. Các phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc khi sao chép, mở các tập tin. 2. Khi gửi văn bản điện tử gửi qua hệ thống thư điện tử phải có định dạng theo Danh mục tiêu chuẩn kỹ thuật về ứng dụng CNTT trong cơ quan nhà nước như: (.txt), (.doc), (.odt), (.pdf) và các định dạng khác theo quy định, không được gửi các file thực thi (.com), (.bat), (.exe)… 3. Các cán bộ, công chức, viên chức và người lao động trong cơ quan phải được hướng dẫn về phòng chống mã độc, các rủi ro do mã độc gây ra; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm trên máy trạm khi chưa có sự đồng ý của người có thẩm quyền theo quy định của cơ quan. 4. Tất cả các máy tính của đơn vị phải được cấu hình nhằm vô hiệu

	hóa tính năng tự động thực thi (autoplay) các tập tin trên các thiết bị lưu trữ di động. 5. Khi phát hiện ra bất kỳ dấu hiện nào liên quan đến việc bị nhiễm mã độc trên máy trạm (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu, …), người sử dụng phải báo trực tiếp cho bộ phận có trách nhiệm của đơn vị để xử lý. 6. Phần mềm ứng dụng trước khi được cài đặt, sử dụng phải được kiểm tra xem có phần mềm độc hại tồn tại hay không? Tất cả các tập tin, thư mục phải được quét mã độc trước khi sao chép, sử dụng. 7. Định kỳ hàng năm thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; Thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống.

5.6. Quản lý giám sát an toàn hệ thống thông tin

Yêu cầu	Có quy định về quản lý giám sát an toàn hệ thống thông tin.
Phương án	Quy định về quản lý giám sát an toàn hệ thống thông tin: 1. Triển khai hệ thống giám sát trung tâm phải đáp ứng yêu cầu tại khoản 1, Điều 5 Thông tư số 31/2017/TT-BTTTT. 2. Thông tin giám sát và danh mục các đối tượng giám sát phải đáp ứng yêu cầu tại khoản 2, Điều 5 Thông tư số 31/2017/TT-BTTTT. Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát. 3. Thực thi nhiệm vụ giám sát theo quy định tại khoản 3, Điều 5 Thông tư số 31/2017/TT-BTTTT. 4. Định kỳ hàng năm tổ chức nâng cao năng lực hoạt động giám sát theo quy định tại Điều 9 Thông tư số 31/2017/TT-BTTTT. 5. Chủ quản hệ thống thông tin có trách nhiệm giám sát an toàn thông tin theo quy định tại Điều 14 Thông tư số 31/2017/TT-BTTTT.

5.7. Quản lý điểm yếu an toàn thông tin

Yêu cầu	Có quy định về quản lý điểm yếu an toàn thông tin.
Phương án	Quy định về quản lý điểm yếu an toàn thông tin:

	1. Đơn vị/bộ phận chuyên trách về an toàn thông tin có trách nhiệm: a) Quản lý thông tin điểm yếu an toàn thông tin đối với từng thành phần có trong hệ thống (hệ điều hành, máy chủ, ứng dụng, dịch vụ…); Phân loại mức độ nguy hiểm của điểm yếu; Xây dựng phương án và quy trình xử lý đối với từng mức độ nguy hiểm của điểm yếu. b) Báo cáo Lãnh đạo/Cán bộ quản lý ngay khi phát hiện điểm yếu an toàn thông tin ở mức độ nghiêm trọng. Thực hiện cảnh báo và xử lý điểm yếu an toàn thông tin theo chỉ đạo. Việc xử lý điểm yếu an toàn thông tin phải bảo đảm không giám ảnh hưởng/gián đoạn hoạt động của hệ thống. c) Xây dựng phương án xử lý tạm thời đối với trường hợp điểm yếu an toàn thông tin chưa được khắc phục và phương án khôi phục hệ thống trong trường hợp xử lý điểm yếu thất bại. d) Có trách nhiệm phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu an toàn thông tin đối với các điểm yếu khi cần thiết. 2. Đối với hệ thống/hệ thống thành phần được đề xuất là cấp độ 3 trở lên phải thực hiện kiểm tra, đánh giá và xử lý điểm yếu an toàn thông tin cho thiết bị hệ thống, máy chủ, dịch vụ trước khi đưa vào sử dụng. 3. Định kỳ hàng năm kiểm tra, đánh giá điểm yếu an toàn thông tin cho toàn bộ hệ thống thông tin; Thực hiện quy trình kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin khi có thông tin hoặc nhận được cảnh báo về điểm yếu an toàn thông tin đối với thành phần cụ thể trong hệ thống. 4. Hoạt động đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thực hiện theo quy định tại điểm c khoản 2 Điều 20 Nghị định số 85/2016/NĐ-CP và Điều 13 Thông tư số 03/2017/TT-BTTTT

5.8. Quản lý sự cố an toàn thông tin

Yêu cầu	Có quy định về quản lý sự cố an toàn thông tin.
Phương án	Quy định về quản lý sự cố an toàn thông tin: 1. Đơn vị/bộ phận chuyên trách về an toàn thông tin có trách nhiệm:

	a) Phân nhóm sự cố an toàn thông tin mạng theo quy định tại Quyết định số 05/2017/NĐ-CP của Thủ tướng Chính phủ ngày 16/3/2017 quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia (Quyết định 05); Xây dựng phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng, ứng phó sự cố an toàn thông tin mạng. b) Xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13,14 Quyết định số 05. c) Xây dựng và triển khai kế hoạch ứng phó sự cố an toàn thông tin theo quy định tại Điều 16 Quyết định số 05. d) Quyết định toàn diện về mặt kỹ thuật đối với các cơ quan trong quá trình khắc phục sự cố về ATTT; Hỗ trợ, phối hợp và hướng dẫn các cơ quan khắc phục sự cố mất ATTT; Yêu cầu ngưng hoạt động một phần hoặc toàn bộ các hệ thống thông tin của các cơ quan nhằm phục vụ công tác khắc phục sự cố về ATTT; Phối hợp với đơn vị chức năng trong điều tra các nguyên nhân gây ra sự cố mất an toàn thông tin theo chỉ đạo của Lãnh đạo. e) Phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin; Yêu cầu bên cung cấp, hỗ trợ cung cấp quy trình xử lý sự cố cho các dịch vụ do bên cung cấp, hỗ trợ cung cấp liên quan đến hệ thống. g) Tổ chức diễn tập phương án xử lý sự cố an toàn thông tin theo chỉ đạo của Lãnh đạo. 2. Trách nhiệm của người dùng: Thông tin, báo cáo kịp thời cho cán bộ chuyên trách về ATTT của cơ quan khi phát hiện các sự cố gây mất ATTT trong quá trình tham gia vào hệ thống thông tin của đơn vị; Phối hợp tích cực trong suốt quá trình giải quyết và khắc phục sự cố.

5.9. Quản lý an toàn người sử dụng đầu cuối

Yêu cầu	Có quy định về quản lý an toàn người sử dụng đầu cuối.
Phương án	Quy định về quản lý an toàn người sử dụng đầu cuối: 1. Kết nối máy tính/thiết bị đầu cuối của người sử dụng vào hệ thống: a) Người sử dụng khi truy cập, sử dụng tài nguyên nội bộ, truy cập mạng và tài nguyên trên Internet phải tuân thủ các quy định của pháp luật về bảo đảm an toàn thông tin và các quy định của cơ quan,

	tổ chức. b) Khi cài đặt, kết nối máy tính/thiết bị đầu cuối phải thực hiện theo hướng dẫn/quy trình dưới sự giám sát của bộ phận chuyên trách về an toàn thông tin. c) Đối với hệ thống thông tin có cấp độ 3 trở lên, máy tính/thiết bị đầu cuối phải được xử lý điểm yếu an toàn thông tin, cấu hình cứng hóa bảo mật trước khi kết nối vào hệ thống. 2. Trong quá trình sử dụng: a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao; b) Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng; c) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách công nghệ thông tin của cơ quan, đơn vị để kịp thời ngăn chặn và xử lý; d) Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng được tỉnh hoặc đơn vị chuyên môn tổ chức.

PHỤ LỤC II. THUYẾT MINH PHƯƠNG ÁN KỸ THUẬT ĐỐI VỚI HỆ THỐNG CỔNG THÔNG TIN NỘI BỘ CẤP ĐỘ 1

Trong Trung tâm tích hợp dữ liệu chỉ có duy nhất 01 hệ thống cổng thông tin nội bộ cấp độ 1. Hệ thống này được triển khai trên các máy chủ Server01 và Server11.

Phương án bảo đảm an toàn thông tin cấp độ 1 cho hai máy chủ này được thuyết minh như dưới đây:

1. Bảo đảm an toàn máy chủ

1.1. Xác thực

Yêu cầu **Máy chủ**	Thiết lập chính sách xác thực trên máy chủ	Thay đổi các tài khoản mặc định trên hệ thống hoặc vô hiệu hóa	Thiết lập chính sách mật khẩu an toàn
Server01/Cài đặt Web-App /Vùng DMZ/HĐH Centos7	+	+	+
Server11/Cài đặt BD/Vùng DB/HĐH Win2k8	+	+	+

1.2. Kiểm soát truy cập

Yêu cầu **Máy chủ**	Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa
Server01/Cài đặt Web-App /Vùng DMZ/HĐH Centos7	+
Server11/Cài đặt BD/Vùng DB/HĐH Win2k8	+

1.3. Nhật ký hệ thống

Yêu cầu **Máy chủ**	Thiết lập lập chức năng ghi nhật ký hệ thống trên các máy chủ	Đồng bộ thời gian giữa máy chủ với máy chủ thời gian
Server01/Cài đặt Web-App /Vùng DMZ/HĐH Centos7	+	+
Server11/Cài đặt BD/Vùng DB/HĐH Win2k8	+	+

1.4. Phòng chống xâm nhập

Yêu cầu	Loại bỏ các tài khoản không sử dụng, các tài khoản không còn hợp lệ trên máy chủ	Sử dụng tường lửa của hệ điều hành và hệ thống để cấm các truy cập trái phép tới máy chủ
Máy chủ		
Server01/Cài đặt Web-App /Vùng DMZ/HĐH Centos7	+	+
Server11/Cài đặt BD/Vùng DB/HĐH Win2k8	+	+

1.5. Phòng chống phần mềm độc hại

Yêu cầu	Cài đặt phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật
Máy chủ	
Server01/Cài đặt Web-App /Vùng DMZ/HĐH Centos7	+
Server11/Cài đặt BD/Vùng DB/HĐH Win2k8	+

2. Bảo đảm an toàn ứng dụng

2.1. Xác thực

Yêu cầu	Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng	Lưu trữ có mã hóa thông tin xác thực hệ thống	Thiết lập cấu hình ứng dụng để đảm bảo an toàn mật khẩu người sử dụng
Ứng dụng			
Cổng thông tin nội bộ	+	+	+

2.2. Kiểm soát truy cập

Yêu cầu	Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị ứng dụng từ xa	Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng
Ứng dụng		
Cổng thông tin nội bộ	+	+

2.3. Nhật ký hệ thống

Yêu cầu	Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau: (1) Thông tin truy cập ứng dụng (2) Thông tin đăng nhập khi quản trị ứng dụng.
Ứng dụng	
Cổng thông tin nội bộ	+

PHỤC LỤC III. THUYẾT MINH PHƯƠNG ÁN KỸ THUẬT ĐỐI VỚI CÁC HỆ THỐNG THÀNH PHẦN CẤP ĐỘ 2

Trong Trung tâm tích hợp dữ liệu chỉ có duy nhất 01 hệ thống quản lý văn bản cấp độ 2. Hệ thống này được triển khai trên các máy chủ Server07 và Server12.

Phương án bảo đảm an toàn thông tin cấp độ 2 cho hai máy chủ này được thuyết minh như dưới đây:

1. Bảo đảm an toàn máy chủ

1.1. Xác thực

Yêu cầu **Máy chủ**	Thiết lập chính sách xác thực trên máy chủ	Thay đổi các tài khoản mặc định trên hệ thống hoặc vô hiệu hóa	Thiết lập chính sách mật khẩu an toàn: Yêu cầu thay đổi mật khẩu mặc định; Thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự; Thiết lập thời gian yêu cầu thay đổi mật khẩu; Thiết lập thời gian mật khẩu hợp lệ
Server07/Cài đặt Web-App/Vùng máy chủ nội bộ/HĐH Centos7	+	+	+
Server12/Cài đặt BD/Vùng DB/HĐH Win2k8	+	+	+

1.2. Kiểm soát truy cập

Yêu cầu **Máy chủ**	Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa	Thiết lập giới hạn thời gian chờ (timeout)
Server07/Cài đặt Web-App/Vùng máy chủ nội bộ/HĐH Centos7	+	+
Server12/Cài đặt BD/Vùng DB/HĐH Win2k8	+	+

1.3. Nhật ký hệ thống

Yêu cầu **Máy chủ**	Thiết lập lập chức năng ghi nhật ký hệ thống trên các máy chủ	Đồng bộ thời gian giữa máy chủ với máy chủ thời gian	Lưu nhật ký hệ thống trong khoảng thời gian tối thiểu là 01 tháng
Server07/Cài đặt Web-App/Vùng máy chủ nội bộ/HĐH Centos7	+	+	+
Server12/Cài đặt BD/Vùng DB/HĐH Win2k8	+	+	+

1.4. Phòng chống xâm nhập

Yêu cầu **Máy chủ**	Loại bỏ các tài khoản không sử dụng, các tài khoản không còn hợp lệ trên máy chủ	Sử dụng tường lửa của hệ điều hành và hệ thống để cấm các truy cập trái phép tới máy chủ	Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ hệ thống không sử dụng	Thực hiện nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng
Server07/Cài đặt Web-App/Vùng máy chủ nội bộ/HĐH Centos7	+	+	+	+
Server12/Cài đặt BD/Vùng DB/HĐH Win2k8	+	+	+	-

1.5. Phòng chống phần mềm độc hại

Yêu cầu **Máy chủ**	Cài đặt phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật	Kiểm tra, dò quét, xử lý phần mềm độc hại cho các phần mềm trước khi cài đặt
Server07/Cài đặt Web-App/Vùng	+	+

máy chủ nội bộ/HĐH Centos7		
Server12/Cài đặt BD/Vùng DB/HĐH Win2k8	+	+

1.6. Xử lý máy chủ khi chuyển giao

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Có phương án xóa sạch thông tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng	Chưa có	Chưa có phương án xử lý máy chủ khi chuyển giao đáp ứng yêu cầu. Sẽ bổ sung phương án, sử dụng giải pháp công nghệ để đáp ứng yêu cầu. Dự kiến thực hiện trước tháng 12/2018.

2. Bảo đảm an toàn ứng dụng

2.1. Xác thực

Yêu cầu / **Ứng dụng**	Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng	Lưu trữ có mã hóa thông tin xác thực hệ thống	Thiết lập cấu hình ứng dụng để đảm bảo an toàn mật khẩu người sử dụng	Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định
Quản lý văn bản	+	+	+	+

2.2. Kiểm soát truy cập

Yêu cầu / **Ứng dụng**	Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị ứng dụng từ xa	Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng	Giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị ứng dụng từ xa
Quản lý văn bản	+	+	+

2.3. Nhật ký hệ thống

Yêu cầu	Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau: (1) Thông tin truy cập ứng dụng (2) Thông tin đăng nhập khi quản trị ứng dụng; (3) Thông tin các lỗi phát sinh trong quá trình hoạt động (4) Thông tin thay đổi cấu hình ứng dụng.	Nhật ký hệ thống phải được lưu trữ trong khoảng thời gian tối thiểu là 01 tháng
Ứng dụng		
Quản lý văn bản	+	+

2.4. An toàn ứng dụng và mã nguồn

Yêu cầu	Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý
Ứng dụng	
Quản lý văn bản	+

PHỤ LỤC IV. THUYẾT MINH PHƯƠNG ÁN KỸ THUẬT ĐỐI VỚI CÁC HỆ THỐNG THÀNH PHẦN CẤP ĐỘ 3

Trung tâm tích hợp dữ liệu có nhiều hệ thống thành phần khác nhau, trong đó hệ thống thành phần cung cấp dịch vụ công trực tuyến được đề xuất là cấp độ 3 (cấp độ cao nhất). Do đó, ngoài các máy chủ được sử dụng để triển khai hệ thống dịch vụ công trực truyến thì các hệ thống dùng chung với các hệ thống thành phần khác trong hệ thống như hạ tầng mạng, hệ thống lưu trữ…được thuyết minh phương án đáp ứng yêu cầu cấp độ 3 như sau:

1. Bảo đảm an toàn mạng

1.1. Thiết kế hệ thống

a) Các vùng mạng trong hệ thống:

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Vùng mạng nội bộ	Không có	Vùng mạng nội bộ độc tập, tách riêng khỏi hệ thống của trung tâm dữ liệu
2	Vùng mạng biên	Có	Kết nối hệ thống với mạng Internet và mạng diện rộng
3	Vùng DMZ	Có	Vùng máy chủ dịch vụ, cung cấp dịch vụ trực tiếp ra bên ngoài Internet
4	Vùng máy chủ nội bộ	Có	Vùng máy chủ nội bộ, cung cấp các dịch vụ nội bộ
5	Vùng mạng máy chủ cơ sở dữ liệu	Có	Lưu trữ và quản lý cơ sở dữ liệu tập trung của các hệ thống thành phần
6	Vùng mạng không dây	Không có	Trung tâm dữ liệu không cho phép sử dụng mạng không dây
7	Vùng quản trị	Có	Chưa thiết kế vùng mạng riêng cho vùng quản trị. Sẽ bổ sung vùng mạng này (Thực hiện trước 12/2018)

b) Phương án bảo đảm an toàn thông tin

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Phương án quản lý truy cập, quản trị hệ thống từ xa an toàn	Có	Các thiết bị hệ thống/máy chủ được thiết lập cấu hình cho phép quản trị từ xa an toàn.
2	Phương án quản lý truy cập giữa các vùng	Có	Truy cập giữa các vùng mạng được quản lý và phòng chống xâm nhập sử dụng các thiết

	mạng và phòng chống xâm nhập		bị tường lửa chuyên dụng có tích hợp chức năng phòng chống xâm nhập.
3	Phương án cân bằng tải và dự phòng nóng cho các thiết bị mạng chính	Có	Các thiết bị mạng chính được thiết kế và cấu hình hoạt động ở chế độ A-A (Thiết kế chi tiết tại sơ đồ vật lý và logic gửi kèm theo).
4	Phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu	Chưa có	Chưa có phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu. Sẽ xây dựng phương án bổ sung (Thực hiện trước 12/2018)
5	Phương án chặn lọc phần mềm độc hại trên môi trường mạng	Chưa có	Chưa có chặn lọc phần mềm độc hại trên môi trường mạng. Sẽ xây dựng phương án bổ sung (Thực hiện trước 12/2018)
6	Phương án phòng chống tấn công từ chối dịch vụ	Có	Hệ thống sử dụng giải pháp của hãng Abor được triển khai ở vùng mạng biên để thực hiện phát hiện và phòng chống tấn công DoS/DDoS
7	Phương án giám sát hệ thống thông tin tập trung	Có	Hệ thống sử dụng giải pháp HP OpenView/Solarwinds/Cacti/Nagios/MRTG để thực hiện giám sát hoạt động của hệ thống mạng, bảo đảm tính khả dụng của hệ thống.
8	Phương án giám sát an toàn hệ thống thông tin tập trung	Có	Hệ thống sử dụng giải pháp ArcSight/Splunk/QRadar/LogRhythm được triển khai ở vùng mạng quản trị, cho phép quản trị tập trung nhật ký hệ thống từ các thiết bị/máy chủ
9	Phương án quản lý sao lưu dự phòng tập trung	Có	Sử dụng hệ thống SAN của hãng HP, có năng lực quản lý và lưu trữ 20T dữ liệu.
10	Có phương án quản lý phần mềm phòng chống mã độc trên các máy chủ/máy tính người dùng tập trung	Chưa có	Chưa có phương án quản lý phần mềm phòng chống mã độc trên các máy chủ/máy tính người dùng tập trung. Sẽ bổ phương án và giải pháp (Thực hiện trước 12/2018).
11	Có phương án phòng, chống thất thoát dữ liệu	Chưa có	Chưa có phương án phòng, chống thất thoát dữ liệu. Sẽ bổ phương án và giải pháp (Thực hiện trước 12/2018).
12	Có phương án dự phòng kết nối mạng Internet cho hệ thống	Có	Sử dụng đồng thời hai kết nối Internet của hai nhà cung cấp dịch vụ khác nhau.

1.2. Kiểm soát truy cập từ bên ngoài mạng

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập thông tin nội bộ hoặc quản trị hệ thống từ các mạng bên ngoài và mạng Internet	Có	Hệ thống được thiết lập chỉ cho phép kết nối mạng có hỗ trợ mã hóa, xác thực khi truy cập thông tin nội bộ hoặc quản trị hệ thống từ các mạng bên ngoài và mạng Internet.
2	Kiểm soát truy cập từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể; chặn tất cả truy cập tới các dịch vụ, ứng dụng mà hệ thống không cung cấp hoặc không cho phép truy cập từ bên ngoài	Có	Hệ thống được thiết lập chỉ cho phép kiểm soát truy cập từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể. Chính sách được thiết lập trên FW01-02 theo chiều từ bên ngoài vào vùng DMZ; trên FW03-04 theo chiều từ bên ngoài vào vùng DB; trên FW07-08 theo chiều từ bên ngoài vào vùng quản trị; trên FW05-06 theo chiều từ bên ngoài vào vùng máy chủ nội bộ.
3	Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi hệ thống không nhận được yêu cầu từ người dùng.	Có	Thiết lập giới hạn thời gian chờ để đóng phiên kết nối khi hệ thống không nhận được yêu cầu từ người dùng được thiết lập trên các FW01-08.
4	Phân quyền và cấp quyền truy cập từ bên ngoài vào hệ thống theo từng người dùng hoặc nhóm người dùng căn cứ theo yêu cầu nghiệp vụ, yêu cầu quản lý.	Có	Thực hiện chính sách trên thiết bị VPN Gateway tại vùng mạng biên. Mỗi người sử dụng sẽ có tài khoản khác nhau, khi kết nối VPN sẽ nhận được địa chỉ IP và chính sách truy cập vào hệ thống khác nhau.
5	Giới hạn số lượng kết nối đồng thời từ một địa chỉ nguồn và tổng số lượng kết nối đồng thời cho từng ứng dụng, dịch vụ được hệ thống cung cấp theo năng lực thực tế của hệ thống	Có	Giới hạn số lượng kết nối đồng thời từ một địa chỉ nguồn và tổng số lượng kết nối đồng thời cho từng ứng dụng, dịch vụ được thiết lập trên các FW01-08.

1.3. Kiểm soát truy cập từ bên trong mạng

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Chỉ cho phép truy cập các ứng dụng, dịch vụ bên ngoài theo yêu cầu nghiệp vụ, chặn các dịch vụ khác không phục vụ hoạt động nghiệp vụ theo chính sách của tổ chức	Có	Chính sách kiểm soát truy cập từ các vùng mạng trong hệ thống đi ra các mạng bên ngoài và mạng Internet được thiết lập trên các cặp tương ứng như kiểm soát truy cập từ bên ngoài trên các FW01-08.
2	Giới hạn truy cập các ứng dụng, dịch vụ bên ngoài theo thời gian	Chưa có	Trung tâm dữ liệu không có vùng mạng nội bộ. Do đó, yêu cầu này sẽ nghiên cứu áp dụng trong trường hợp cụ thể.
3	Có phương án kiểm soát truy cập của người dùng vào các dịch vụ, các máy chủ nội bộ theo chức năng và chính sách của tổ chức	Chưa có	Trung tâm dữ liệu không có vùng mạng nội bộ. Do đó, yêu cầu này sẽ nghiên cứu áp dụng trong trường hợp cụ thể.

1.4. Nhật ký hệ thống

Yêu cầu **Thiết bị**	Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên các thiết bị hệ thống	Sử dụng máy chủ thời gian trong hệ thống để đồng bộ thời gian	Lưu trữ và quản lý tập trung nhật ký hệ thống	Lưu trữ nhật ký hệ thống của thiết bị tối thiểu 03 tháng
FW01	+	+	+	+
FW02	+	+	+	-
FW03	+	+	+	+
FW04	+	+	+	-
FW05	+	+	+	+
FW06	+	+	+	-
FW07	+	+	+	+
FW08	+	+	+	-
CW01	+	+	-	-
CW01	+	+	-	-
AntiDDoS	+	+	-	-
VPN Gateway	+	+	+	-

1.5. Phòng chống xâm nhập

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Có phương án phòng chống xâm nhập để bảo vệ các vùng mạng trong hệ thống	Có	Các vùng mạng được triển khai hệ thống IDS/IPS, hoạt động ở chế độ Inline cho phép phát hiện và phòng chống xâm nhập.
2	Định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng	Có	Đã thiết lập chức năng tự động cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng đều được thiết lập trên các thiết bị IDS/IPS.
3	Bảo đảm năng lực hệ thống đáp ứng đủ theo yêu cầu, quy mô số lượng người dùng và dịch vụ, ứng dụng của hệ thống cung cấp	Có	Các IDS/IPS có năng lực xử lý đáp ứng đủ theo yêu cầu, quy mô số lượng người dùng và dịch vụ, ứng dụng của hệ thống cung cấp.

1.6. Phòng chống phần mềm độc hại trên môi trường mạng

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Có phương án phòng chống phần mềm độc hại trên môi trường mạng	Có	Chức năng phòng chống phần mềm độc hại trên môi trường mạng được tích hợp trên các Firewall. Các Firewall được thiết lập cấu hình để có thể phát hiện ra các hành vi mã độc trên môi trường mạng.
2	Định kỳ cập nhật dữ liệu cho hệ thống phòng chống phần mềm độc hại	Có	Đã thiết lập chức năng cập nhật dữ liệu cho hệ thống phòng chống phần mềm độc hại trên các Firewall có tích hợp chức năng phòng chống phần mềm độc hại trên môi trường mạng.
3	Bảo đảm năng lực hệ thống đáp ứng đủ theo yêu cầu, quy mô số lượng người dùng và dịch vụ, ứng dụng của hệ thống cung cấp	Có	Các các Firewall có tích hợp chức năng phòng chống phần mềm độc hại trên môi trường mạng có năng lực xử lý đáp ứng đủ theo yêu cầu, quy mô số lượng người dùng và dịch vụ, ứng dụng của hệ thống cung cấp.

1.7. Bảo vệ thiết bị hệ thống

Yêu cầu / **Thiết bị**	Cấu hình chức năng xác thực trên các thiết bị	Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị thiết bị từ xa	Hạn chế các địa chỉ mạng có thể kết nối, quản trị thiết bị từ xa	Hạn chế được số lần đăng nhập sai	Phân quyền truy cập, quản trị thiết bị	Nâng cấp, xử lý điểm yếu an toàn thông tin của thiết bị hệ thống trước khi đưa vào sử dụng
FW01	+	+	+	+	+	+
FW02	+	+	+	+	+	+
FW03	+	+	-	-	-	-
FW04	+	+	-	-	-	+
FW05	+	+	-	-	-	+
FW06						
FW07	+	+	+	+	+	+
FW08	+	+	+	+	+	+
CW01	+	+	-	-	-	-
CW01	+	+	-	-	-	+
AntiDDoS	+	+	-	-	-	+

2. Bảo đảm an toàn máy chủ

2.1. Xác thực

Yêu cầu / **Máy chủ**	Thiết lập chính sách xác thực trên máy chủ	Thay đổi các tài khoản mặc định trên hệ thống hoặc vô hiệu hóa	Thiết lập chính sách mật khẩu an toàn	Hạn chế số lần đăng nhập sai	vô hiệu hóa tài khoản nếu tài khoản đó đăng nhập sai nhiều lần vượt số lần quy định
Server02/Cài đặt Reserver Proxy/Vùng DMZ/HĐH Centos7	+	+	+	+	+

Server06/Cài đặt Web-App/Vùng máy chủ nội bộ/HĐH Centos7	+	+	+	-	+
Server10/Cài đặt BD/Vùng DB/HĐH Centos	+	+	-	-	-

2.2. Kiểm soát truy cập

Yêu cầu **Máy chủ**	Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa	Thiết lập giới hạn thời gian chờ (timeout)	Thay đổi cổng quản trị mặc định của máy chủ	Giới hạn địa chỉ mạng được phép truy cập, quản trị máy chủ từ xa
Server02/Cài đặt Reserver Proxy/Vùng DMZ/HĐH Centos7	+	+	+	+
Server06/Cài đặt Web-App/Vùng máy chủ nội bộ/HĐH Centos7	+	+	+	-
Server10/Cài đặt BD/Vùng DB/HĐH Centos	+	+	-	-

2.3. Nhật ký hệ thống

Yêu cầu **Máy chủ**	Thiết lập lập chức năng ghi nhật ký hệ thống trên các máy chủ	Đồng bộ thời gian giữa máy chủ với máy chủ thời gian	Giới hạn đủ dung lượng lưu trữ nhật ký hệ thống để không mất hoặc tràn nhật ký hệ thống	Quản lý và lưu trữ tập trung nhật ký hệ thống thu thập được từ máy chủ	Lưu nhật ký hệ thống trong khoảng thời gian tối thiểu là 03 tháng
Server02/Cài đặt Reserver Proxy/Vùng DMZ/HĐH Centos7	+	+	+	+	+
Server06/Cài đặt Web-App/Vùng máy chủ nội bộ/HĐH Centos7	+	+	+	-	+
Server10/Cài đặt BD/Vùng DB/HĐH Centos	+	+	-	-	-

2.4. Phòng chống xâm nhập

Yêu cầu **Máy chủ**	Loại bỏ các tài khoản không sử dụng, các tài khoản không còn hợp lệ trên máy chủ	Sử dụng tường lửa của hệ điều hành và hệ thống để cấm các truy cập trái phép tới máy chủ	Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ hệ thống không sử dụng	Thực hiện nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng
Server02/Cài đặt Reserver Proxy/Vùng DMZ/HĐH Centos7	+	+	+	+

Server06/Cài đặt Web-App/Vùng máy chủ nội bộ/HĐH Centos7	+	+	+	-
Server10/Cài đặt BD/Vùng DB/HĐH Centos	+	+	-	-

2.5. Phòng chống phần mềm độc hại

Yêu cầu / **Máy chủ**	Cài đặt phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật	Kiểm tra, dò quét, xử lý phần mềm độc hại cho các phần mềm trước khi cài đặt	Quản lý tập trung các phần mềm phòng chống mã độc cài đặt trên máy chủ
Server02/Cài đặt Reserver Proxy/Vùng DMZ/HĐH Centos7	+	+	-
Server06/Cài đặt Web-App/Vùng máy chủ nội bộ/HĐH Centos7	+	+	-
Server10/Cài đặt BD/Vùng DB/HĐH Centos	+	+	-

2.6. Xử lý máy chủ khi chuyển giao

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Có phương án xóa sạch thông tin,	Chưa	Chưa có phương án xử lý máy

	dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng	có	chủ khi chuyển giao đáp ứng yêu cầu. Sẽ bổ sung phương án, sử dụng giải pháp công nghệ để đáp ứng yêu cầu. Dự kiến thực hiện trước tháng 12/2018.
2	Sao lưu dự phòng thông tin, dữ liệu trên máy chủ, bản dự phòng hệ điều hành máy chủ trước khi thực hiện xóa dữ liệu, hệ điều hành	Chưa có	
3	Có biện pháp kiểm tra, bảo đảm dữ liệu không thể khôi phục sau khi xóa	Chưa có	

3. Bảo đảm an toàn ứng dụng

3.1. Xác thực

Yêu cầu **Ứng dụng**	Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng	Lưu trữ có mã hóa thông tin xác thực hệ thống	Thiết lập cấu hình ứng dụng để đảm bảo an toàn mật khẩu người sử dụng	Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định	Mã hóa thông tin xác thực trước khi gửi qua môi trường mạng	Thiết lập cấu hình ứng dụng để ngăn cản việc đăng nhập tự động đối với các ứng dụng
Dịch vụ công trực tuyến	+	+	+	+	+	-

3.2. Kiểm soát truy cập

Yêu cầu	Chỉ cho phép sử dụng các kết nối mạng an	Thiết lập giới hạn thời gian chờ (timeout) để	Giới hạn địa chỉ mạng quản trị được phép truy	Phân quyền truy cập, quản trị, sử dụng tài nguyên	Giới hạn số lượng các kết nối đồng thời (kết nối

Ứng dụng	toàn khi truy cập, quản trị ứng dụng từ xa	đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng	cập, quản trị ứng dụng từ xa	khác nhau của ứng dụng với từng người/nhóm sử dụng	khởi tạo và đã thiết lập) đối với các ứng dụng
Dịch vụ công trực tuyến	+	+	+	+	+

3.3. Nhật ký hệ thống

Yêu cầu	Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau: (1) Thông tin truy cập ứng dụng (2) Thông tin đăng nhập khi quản trị ứng dụng; (3) Thông tin các lỗi phát sinh trong quá trình hoạt động (4) Thông tin thay đổi cấu hình ứng dụng	Quản lý và lưu trữ nhật ký hệ thống trên hệ thống quản lý tập trung	Nhật ký hệ thống phải được lưu trữ trong khoảng thời gian tối thiểu là 03 tháng
Ứng dụng			
Dịch vụ công trực tuyến	+	+	+

3.4. Bảo mật thông tin liên lạc

Yêu cầu	Mã hóa thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trước khi truyền đưa, trao đổi qua môi trường mạng; sử dụng phương án mã hóa theo quy định về bảo vệ bí mật nhà nước đối với thông tin mật.	Sử dụng kết nối mạng an toàn, bảo đảm an toàn trong quá trình khởi tạo kết nối kênh truyền và trao đổi thông tin qua kênh truyền
Ứng dụng		
Dịch vụ công trực tuyến	+	+

3.5. Chống chối bỏ

Yêu cầu	Sử dụng chữ ký số khi trao đổi thông tin, dữ liệu quan trọng
Ứng dụng	
Dịch vụ công trực tuyến	+

3.6. An toàn ứng dụng và mã nguồn

Yêu cầu	Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý	Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu ra trước khi gửi về máy yêu cầu	Giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị ứng dụng từ xa	Có phương án bảo vệ ứng dụng chống lại những dạng tấn công phổ biến: SQL Injection, OS command injection, RFI, LFI, Xpath injection, XSS, CSRF
Ứng dụng				
Dịch vụ công trực tuyến	+	+	+	-

4. Bảo đảm an toàn dữ liệu

4.1. Nguyên vẹn dữ liệu

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Có phương án quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã kiểm tra tính nguyên vẹn	Có	Dữ liệu quan trọng trên hệ thống bao gồm dữ liệu: dữ liệu nghiệp vụ, văn bản điện tử quan trọng và dữ liệu cấu hình hệ thống. Dữ liệu được nén và được lưu trữ cùng mã kiểm tra MD5 trên hệ thống SAN.

4.2. Bảo mật dữ liệu

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Lưu trữ có mã hóa các thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trên hệ thống lưu trữ/phương tiện lưu trữ	Có	Dữ liệu quan trọng trên hệ thống bao gồm dữ liệu: dữ liệu nghiệp vụ, văn bản điện tử quan trọng và dữ liệu cấu hình hệ thống. Dữ liệu được nén và được lưu

			trữ mã hóa sử dụng công cụ XXX (hỗ trợ các chuẩn mã hóa: DES, AES…) trên hệ thống SAN.

4.3. Sao lưu dự phòng

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Thực hiện sao lưu dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ	Có	Thông tin, dữ liệu được lưu trữ và quản lý tập trung trên hệ thống lưu trữ SAN.
2	Phân loại và quản lý các dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau	Có	Thông tin dữ liệu được phân theo từng nhóm theo đặc trưng nghiệp vụ hoặc chức năng. Được quy định về việc đặt tên các tập tin/thư mục khi lưu trữ trên hệ thống.
3	Có hệ thống/phương tiện lưu trữ độc lập để sao lưu dự phòng	Có	Hệ thống SAN được phân vùng lưu trữ riêng để phục vụ việc lưu trữ thông tin, dữ liệu.

PHỤ LỤC II
HỒ SƠ ĐỀ XUẤT CẤP ĐỘ MẪU CHO HỆ THỐNG THƯ ĐIỆN TỬ

ỦY BAN NHÂN DÂN TỈNH B
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

HỒ SƠ MẪU

HỒ SƠ ĐỀ XUẤT CẤP ĐỘ CHO HỆ THỐNG THƯ ĐIỆN TỬ CỦA TỈNH B

Tỉnh B - 2019

THUẬT NGỮ, TỪ VIẾT TẮT

STT	Từ viết tắt	Nghĩa đầy đủ
1.	CNTT	Công nghệ thông tin
2.	CSDL	Cơ sở dữ liệu
3.	DVCTT	Dịch vụ công trực tuyến
4.	MCĐT	Một cửa điện tử
5.	WAN	Mạng tin học diện rộng
6.	LAN	Mạng nội bộ
7.	TSLCD	Mạng Truyền số liệu chuyên dùng
8.	VPN	Vitural Private Network
9.	DNS	Domain Name Server

PHẦN I. THÔNG TIN TỔNG QUAN VỀ HỆ THỐNG THƯ ĐIỆN TỬ

1. Thông tin Chủ quản hệ thống thông tin

- Tên tổ chức: UBND Tỉnh B
- Quy định chức năng, nhiệm vụ và quyền hạn: …
- Người đại diện: Ông/Bà Trần Văn A, Chức vụ: Chủ tịch UBND Tỉnh.
- Địa chỉ: Số… đường ……, tỉnh B
- Số điện thoại: …., email: vpubndtinh@tinhb.gov.vn.

2. Thông tin Đơn vị vận hành

- Tên Đơn vị vận hành: Sở Thông tin và Truyền Thông tỉnh B
- Quy định chức năng, nhiệm vụ và quyền hạn: Quyết định số ...
- Người đại diện: Ông Nguyễn Văn B, Chức vụ: Giám đốc.
- Địa chỉ: Số… đường ……, tỉnh B
- Số điện thoại: …, email: stttt@tinhb.gov.vn.

3. Mô tả phạm vi, quy mô của hệ thống

3.1. Phạm vi:

Hệ thống thư điện tử là thành phần của hệ thống thông tin điện tử quản lý hành chính nhà nước của UBND tỉnh B. Hệ thống thư điện tử được kết nối trực tuyến với mạng Internet cho phép gửi, nhận thông tin dưới dạng thư điện tử phục vụ công tác chuyên môn, nghiệp vụ của các cơ quan, đơn vị, cán bộ, công chức, viên chức, cá nhân, doanh nghiệp của tỉnh.

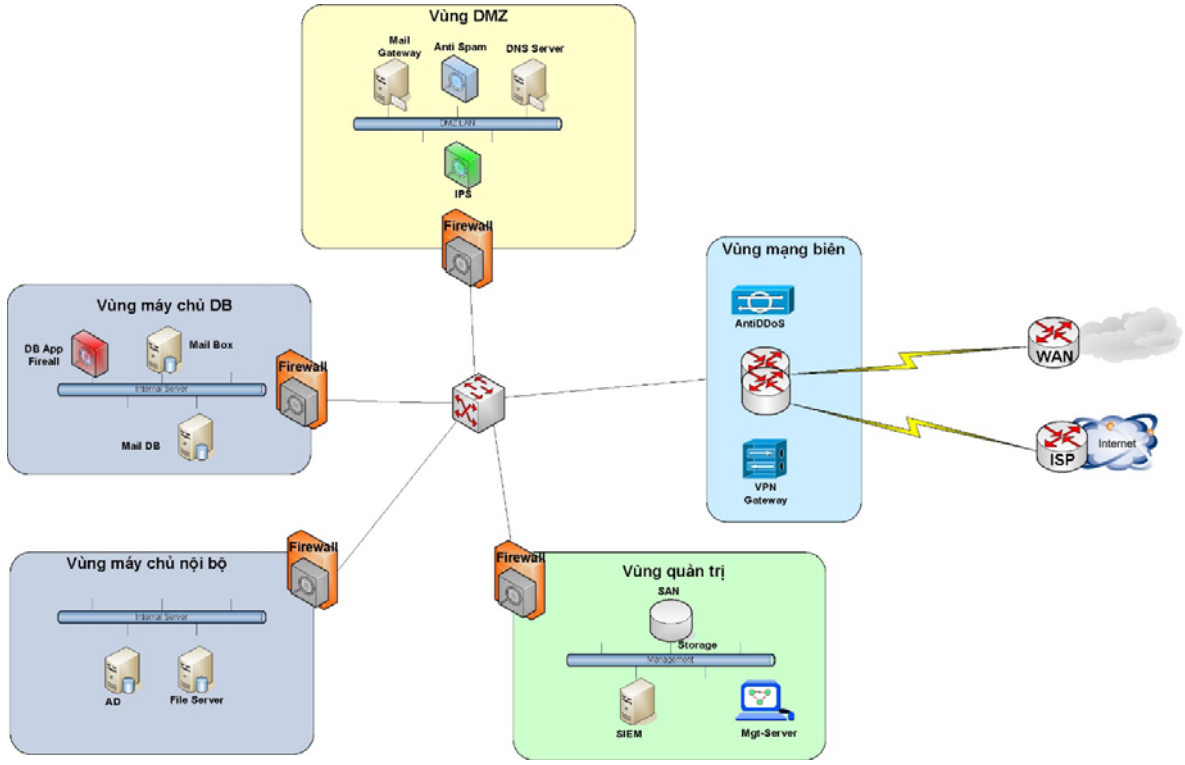
Hệ thống thư điện tử có tên miền là: @ tinhb.gov.vn và địa chỉ truy cập trên internet là: mail.tinhb.gov.vn.

3.2. Quy mô:

Hệ thống thư điện tử có quy mô phục vụ các cơ quan, đơn vị, cán bộ, công chức, viên chức, cá nhân, doanh nghiệp của tỉnh với quy mô hơn 10.000 người sử dụng.

4. Mô tả cấu trúc của hệ thống

4.1. Sơ đồ logic tổng thể



Hình 1: Cấu trúc logic các thành phần của hệ thống thư điện tử

Các vùng mạng được thiết kế như sau:

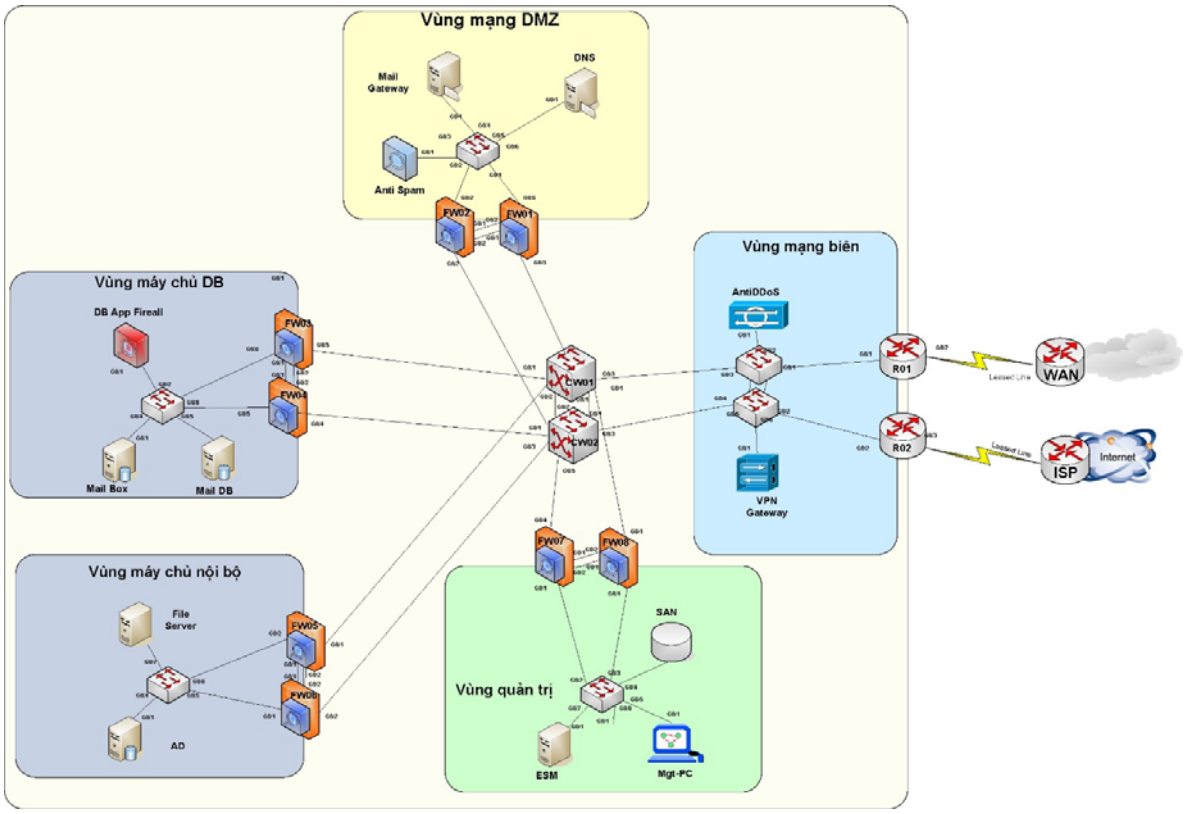
+ Vùng mạng biên được thiết kế để kết nối hệ thống thư điện tử ra các mạng bên ngoài và mạng Internet; bảo vệ hệ thống thư điện tử từ bên ngoài Internet. Vùng mạng này triển khai hệ thống phòng chống tấn công DDoS và Thiết bị cung cấp cổng kết nối VPN.

+ Vùng DMZ đặt các máy chủ Mail Gateway, DNS để 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 AD phục vụ xác thực người sử dụng và máy chủ File Server. Vùng mạng này triển khai thiết bị phòng chống xâm nhập IPS, thiết bị Web Application Firewall, thiết bị tường lửa cho CSDL…

4.2. Sơ đồ kết nối vật lý



Hình 2: Kết nối vật lý các thành phần của hệ thống thư điện tử

4.3. Danh mục thiết bị sử dụng trong hệ thống

Bảng 1: Danh mục thiết bị sử dụng trong hệ thống

STT	Tên thiết bị/ Chủng loại	Vị trí triển khai	Mục đích sử dụng
1	R01/Cisco3800	Vùng mạng biên	Kết nối và định tuyến động với các Router của 02 ISP.
2	R02/Cisco3800	Vùng mạng biên	Kết nối và định tuyến động với các Router của 02 ISP (Dự phòng nóng cho R01).
3	FW01/ASA5505	Vùng DMZ	Quản lý truy cập vào/ra và bảo vệ vùng mạng DMZ.
4	FW02/ASA5505	Vùng DMZ	Quản lý truy cập vào/ra và bảo vệ vùng mạng (Dự phòng nóng cho FW01).
5	FW03/Fortigate100C	Vùng máy chủ DB	Quản lý truy cập vào/ra và bảo vệ vùng máy chủ DB.

6	FW04/Fortigate100C	Vùng máy chủ DB	Quản lý truy cập vào/ra và bảo vệ vùng máy chủ DB (Dự phòng nóng cho FW03) ...
7	Anti Spam	Vùng DMZ	Lọc thư rác cho hệ thống thư điện tử
8	DB App Firewall	Vùng máy chủ DB	Tường lửa lớp mạng cho máy chủ DB.

4.4. Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống

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

STT	Tên dịch vụ	Máy chủ/Ứng dụng cài đăt/Vùng mạng/HĐH	Mục đích sử dụng
1	Hệ thống thư điện tử	1) Server01/Cài đặt Mail Gatteway/Vùng DMZ/HĐH Centos7 2) Server02/Cài đặt Mail Box/Vùng máy chủ nội bộ/HĐH Centos7 3) Server3/Cài đặt hệ quản trị cơ sở dữ liệu cho Mail Server/Vùng DB/HĐH Win2k8 4) Server4/Cài đặt máy chủ xác thực AD/Vùng DB/HĐH Win2k8 5) Server05/Cài đặt File Server /Vùng máy chủ nội bộ/HĐH Centos7	Cung cấp dịch vụ thư điện tử cho cán bộ trên địa bàn tỉnh B.

4.5. Quy hoạch địa chỉ IP các vùng mạng trong hệ thống

Bảng 3: Các vùng mạng trong hệ thống

STT	Vùng mạng	IP Private	IP Public
1	DMZ	192.168.1.0/24	202.191.x.0/24
2	Vùng mạng quản trị	192.168.2.0/24	202.191.y.0/24
3	Vùng máy chủ nội bộ	192.168.3.0/24	202.191.z.0/24
4	Vùng máy chủ CSDL	…	

PHẦN II. THUYẾT MINH CẤP ĐỘ ĐỀ XUẤT

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

Hệ thống thông tin thuộc phạm vi quản lý của Tổ chức A bao gồm các hệ thống thành phần với cấp độ đề xuất tương ứng, bao gồm:

STT	Hệ thống	Cấp độ đề xuất	Căn cứ đề xuất
1	Hệ thống thư điện tử	3	Điểm c, khoản 2, Điều 9, NĐ85

2. Thuyết minh đề xuất cấp độ đối với hệ thống thư điện tử

Hệ thống thư điện tử là thành phần của hệ thống thông tin điện tử quản lý hành chính nhà nước của UBND tỉnh B. Hệ thống thư điện tử được kết nối trực tuyến với mạng Internet cho phép gửi, nhận thông tin dưới dạng thư điện tử phục vụ công tác chuyên môn, nghiệp vụ của các cơ quan, đơn vị, cán bộ, công chức, viên chức, cá nhân, doanh nghiệp của tỉnh.

Hệ thống thư điện tử có quy mô phục vụ các cơ quan, đơn vị, cán bộ, công chức, viên chức, cá nhân, doanh nghiệp của tỉnh với quy mô hơn 10.000 người sử dụng...

Hệ thông thư điện tử có xử lý thông tin riêng của người sử dụng hoặc thông tin riêng của tổ chức trong các hoạt động chỉ đạo, điều hành của tỉnh.

Trên cơ sở đó, hệ thống thư điện tử được xác định là **cấp độ 3** căn cứ theo tiêu chí xác định cấp độ tại Điều 9, khoản 2, điểm c, Nghị định 85/2016/NĐ-CP.

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

Phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử phải bảo đảm đáp ứng các yêu cầu an toàn về quản lý và kỹ thuật đối với hệ thống thông tin cấp độ 3, được thuyết minh như dưới đây.

Đối với thuyết minh phương án quản lý, thuyết minh đưa ra các phương án để thực hiện nhằm đáp ứng các yêu cầu an toàn về quản lý. Trường hợp, quy chế, chính sách bảo đảm an toàn thông tin của tổ chức hiện tại chưa đáp ứng các yêu cầu như phương án đề xuất, thì thuyết minh đưa ra lộ trình thực hiện cập nhật, bổ sung quy chế, chính sách hiện hành nhằm đáp ứng các yêu cầu về quản lý, bao gồm:

- Quy chế bảo đảm an toàn thông tin
- Tổ chức bảo đảm an toàn thông tin
- Bảo đảm nguồn nhân lực an toàn thông tin
- Quản lý thiết kế, xây dựng hệ thống thông tin
- Quản lý vận hành hệ thống thông tin

Đối với thuyết minh phương án kỹ thuật, thuyết minh chỉ ra phương án, hiện trạng cấu hình và thiết lập hệ thống đã đáp ứng các yêu cầu an toàn về kỹ thuật. Trường hợp, phương án kỹ thuật, hiện trạng cấu hình và thiết lập hệ thống chưa đáp ứng các yêu cầu an toàn về quản lý, thì thuyết minh sẽ đưa ra phương án, lộ trình để nâng cấp, điều chỉnh hệ thống nhằm đáp ứng các yêu cầu an toàn về kỹ thuật, bao gồm:

- Bảo đảm an toàn mạng
- Bảo đảm an toàn máy chủ
- Bảo đảm an toàn ứng dụng
- Bảo đảm an toàn dữ liệu

Các yêu cầu an toàn về quản lý sẽ được cập nhật bổ sung để đáp ứng yêu cầu đặt ra trong vòng 06 tháng kể từ khi HSĐXCĐ được phê duyệt.

Các yêu cầu an toàn về kỹ thuật sẽ được cập nhật bổ sung để đáp ứng yêu cầu đặt ra trong vòng 18 tháng kể từ khi HSĐXCĐ được phê duyệt.

I. Thuyết minh phương án đáp ứng yêu cầu quản lý

1. Xây dựng quy chế bảo đảm an toàn thông tin

1.1. Quy chế bảo đảm an toàn thông tin

Yêu cầu	Xác định các mục tiêu, nguyên tắc bảo đảm an toàn thông tin.
Phương án	Mục tiêu: Quy chế bảo đảm an toàn thông tin được xây dựng nhằm thống nhất cấu trúc hệ thống quản lý an ninh thông tin của hệ thống thư điện tử, nêu ra các yêu cầu cơ bản nhất về hệ thống, mô tả các mối tương tác trong tiêu chuẩn quốc gia TCVN 11930. Nguyên tắc bảo đảm an toàn thông tin: 1. Việc bảo đảm an toàn thông tin (ATTT) là yêu cầu bắt buộc trong quá trình tạo lập, xử lý, sử dụng thông tin và quá trình thiết kế, xây dựng, vận hành, nâng cấp, hủy bỏ hệ thống thư điện tử. 2. Các cơ quan, đơn vị và cá nhân có trách nhiệm đảm bảo ATTT theo quy định của Nhà nước, của UBND và hướng dẫn của các cơ quan, đơn vị có thẩm quyền trong lĩnh vực ATTT. 3. Người dùng phải được tập huấn, phổ biến kiến thức cơ bản về ATTT trên môi trường máy tính, mạng máy tính và kiến thức nâng cao đối với cán bộ chuyên môn. 4. Thông tin thuộc danh mục bí mật nhà nước trên môi trường máy tính và mạng máy tính phải được bảo vệ theo các quy định của Nhà nước và các nội dung tương ứng trong quy định này. 5. Giảm thiểu các nguy cơ gây mất ATTT trong sử dụng hệ thống thư điện tử. 6. Đảm bảo tính bảo mật a) Đảm bảo thông tin chỉ có thể được truy cập bởi những đối tượng (người, chương trình máy tính...) được cấp quyền truy cập. b) Mật khẩu truy cập, khóa mã hóa và các mã khóa khác được mã hóa trong quá trình truy cập, trên đường truyền và lưu trữ tại đơn vị quản lý thông tin. 7. Đảm bảo tính nguyên vẹn a) Đảm bảo tính nguyên vẹn thông tin là việc thông tin chỉ được phép xóa hoặc sửa bởi những đối tượng được phép và phải đảm bảo rằng nội dung thư điện tử vẫn còn chính xác khi được lưu trữ hay truyền đi. b) Việc quản lý, sử dụng, lưu trữ, truyền đưa các thông tin phải đảm bảo tính nguyên vẹn, không được thay đổi khi chưa được phép của đơn vị quản lý thông tin.

	c) Việc đảm bảo tính nguyên vẹn phải được thực hiện trong toàn bộ các quá trình truy cập, các quá trình nhập, lưu trữ, sử dụng, xử lý, truyền tải, trích rút và khôi phục dữ liệu. 8. Đảm bảo tính khả dụng a) Đảm bảo khả năng hoạt động liên tục của hệ thống thông tin. b) Đảm bảo thông tin phải được truy cập nhanh chóng khi có sự yêu cầu từ phía cá nhân, tổ chức được cho phép truy cập thông tin. c) Đảm bảo nguồn nhân lực trong việc vận hành hệ thống thông tin.
Yêu cầu	Xác định trách nhiệm của đơn vị chuyên trách về an toàn thông tin, các cán bộ làm về an toàn thông tin và các đối tượng thuộc phạm vi điều chỉnh của chính sách an toàn thông tin.
Phương án	Quy định trách nhiệm của cơ quan, tổ chức trên địa bàn trong công tác bảo đảm an toàn thông tin: 1. UBND tỉnh B có trách nhiệm thực hiện các nhiệm vụ của chủ quản hệ thống thông tin đối với các hệ thống thông tin trên địa bàn theo quy định tại Điều 20, Nghị định 85/2016/NĐ-CP. 2. Trách nhiệm của Sở Thông tin và Truyền thông a) Tham mưu Ủy ban nhân dân tỉnh và Ban chỉ đạo công tác bảo đảm an toàn thông tin mạng trên địa bàn tỉnh. b) Thực hiện trách nhiệm của đơn vị chuyên trách về an toàn thông tin theo quy định của pháp luật theo quy định tại Điều 21, Nghị định 85/2016/NĐ-CP. c) Thực hiện trách nhiệm của đơn vị vận hành đối với các hệ thống thông tin thuộc phạm vi quản lý. d) Làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng trên địa bàn tỉnh. e) Chủ trì, phối hợp với Văn phòng Ủy ban nhân dân tỉnh, Công an tỉnh và các đơn vị có liên quan tiến hành kiểm tra công tác bảo đảm an toàn thông tin mạng định kỳ hàng năm hoặc theo chỉ đạo của UBND tỉnh đối với các cơ quan nhà nước trong tỉnh. g) Tùy theo mức độ sự cố, phối hợp Cục An toàn thông tin hoặc Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam và các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố an toàn thông tin mạng.

	h) Tổng hợp và báo cáo về tình hình an toàn thông tin mạng theo định kỳ cho Bộ Thông tin và Truyền thông, Ủy ban nhân dân tỉnh theo quy định của pháp luật. i) Hàng năm, xây dựng và triển khai các chương trình đào tạo, tập huấn về công tác bảo đảm an toàn thông tin mạng cho cán bộ, công chức phụ trách an toàn thông tin mạng của các cơ quan, đơn vị. Tổ chức các hội nghị, hội thảo chuyên đề và tuyên truyền về an toàn thông tin mạng trong công tác quản lý nhà nước trên địa bàn tỉnh. k) Tổ chức tuyên truyền, hướng dẫn về công tác bảo đảm an toàn thông tin mạng. l) Phối hợp với Ban Tuyên giáo Tỉnh ủy, Công an tỉnh có các biện pháp phòng, chống các thông tin vi phạm pháp luật, ảnh hưởng đến an ninh quốc gia, trật tự, an toàn xã hội trên môi trường mạng, nhất là trên các cổng/trang thông tin điện tử, mạng xã hội. 3. Trách nhiệm của các cơ quan, đơn vị a) Thủ trưởng các cơ quan, đơn vị có trách nhiệm tổ chức thực hiện các quy định tại quy chế này và chịu trách nhiệm trong công tác bảo đảm an toàn thông tin mạng của cơ quan, đơn vị mình. b) Thực hiện trách nhiệm của đơn vị vận hành theo quy định tại Điều 22, Nghị định 85/2016/NĐ-CP. c) Phân công một bộ phận hoặc cán bộ phụ trách bảo đảm an toàn thông tin mạng của đơn vị, tạo điều kiện để các cán bộ được học tập, nâng cao trình độ về an toàn thông tin mạng. d) Bố trí, tạo điều kiện làm việc cho cán bộ chuyên trách về công nghệ thông tin trong các cơ quan, đơn vị phù hợp với chuyên môn, được ưu tiên bồi dưỡng nghiệp vụ về an toàn thông tin mạng. e) Xây dựng quy chế, quy trình về bảo đảm an toàn thông tin mạng phù hợp với quy chế này và các quy định của pháp luật. g) Phối hợp, cung cấp thông tin và tạo điều kiện cho các đơn vị có thẩm quyền triển khai công tác kiểm tra khắc phục sự cố xảy ra một cách kịp thời, nhanh chóng và đạt hiệu quả. h) Phối hợp chặt chẽ với Sở Thông tin và Truyền thông, Công an tỉnh trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin mạng.

	i) Khuyến khích các cơ quan, đơn vị liên kết các tổ chức, cá nhân, doanh nghiệp CNTT mở các khóa đào tạo nhân lực trong lĩnh vực an toàn thông tin mạng mạng. k) Hàng năm bố trí kinh phí cho việc ứng dụng công nghệ thông tin nói chung và công tác bảo đảm an toàn thông tin mạng nói riêng trong nội bộ cơ quan, đơn vị mình; lập kế hoạch nâng cấp, bảo trì, sửa chữa, gia hạn bản quyền phần mềm... cho các hệ thống phần cứng, phần mềm nhằm thực hiện tốt công tác bảo mật, bảo đảm an toàn thông tin mạng đưa vào dự toán chi năm sau để triển khai thực hiện. 4. Trách nhiệm của cán bộ, công chức, viên chức và người lao động trong các cơ quan, đơn vị a) Trách nhiệm của bộ phần chuyên trách về an toàn thông tin: i) Chịu trách nhiệm bảo đảm an toàn thông tin mạng của cơ quan, đơn vị; ii) Tham mưu lãnh đạo cơ quan ban hành các quy chế, quy trình nội bộ, triển khai các giải pháp kỹ thuật bảo đảm an toàn thông tin mạng; iii) Thực hiện việc giám sát, đánh giá, báo cáo Thủ trưởng cơ quan, đơn vị các rủi ro mất an toàn thông tin mạng và mức độ nghiêm trọng của các rủi ro đó; iv) Phối hợp với các cá nhân, đơn vị có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn thông tin mạng; v) Thường xuyên cập nhật nâng cao kiến thức, trình độ chuyên môn đáp ứng yêu cầu bảo đảm an toàn thông tin mạng của đơn vị. b) Trách nhiệm của người sử dụng: i) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao; ii) Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng; iii) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách công nghệ thông tin của cơ quan, đơn vị để kịp thời ngăn chặn và xử lý;

	iv) Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng được tỉnh hoặc đơn vị chuyên môn tổ chức.

1.2. Xây dựng và công bố

Yêu cầu	Quy định về xây dựng và công bố quy chế bảo đảm an toàn thông tin.
Phương án	Xây dựng và công bố quy chế bảo đảm an toàn thông tin: 1: Quy chế được tổ chức/bộ phận được ủy quyền thông qua trước khi công bố áp dụng 2: Quy chế được Sở TT&TT xây dựng trình Chủ tịch UBND tỉnh B ban hành.

1.3. Rà soát, sửa đổi

Yêu cầu	Có quy định về việc rà soát, sửa đổi quy chế bảo đảm an toàn thông tin.
Phương án	Rà soát, sửa đổi quy chế bảo đảm an toàn thông tin: 1. Định kỳ 02 năm hoặc khi có thay đổi quy chế bảo đảm an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung. 2. Trong quá trình thực hiện quy chế, nếu có vấn đề vướng mắc, phát sinh, các đơn vị phản ánh kịp thời về Sở Thông tin và Truyền thông để tổng hợp báo cáo Uỷ ban nhân dân tỉnh điều chỉnh, bổ sung...

2. Tổ chức bảo đảm an toàn thông tin

2.1. Đơn vị chuyên trách về an toàn thông tin

Yêu cầu	Thành lập hoặc chỉ định đơn vị/bộ phận chuyên trách về an toàn thông tin trong tổ chức.
Phương án	Sở TT&TT xây dựng dự thảo Quyết định giao Sở TT&TT là đơn vị chuyên trách về an toàn thông tin, trình Chủ tịch UBND tỉnh B ban hành. Phòng CNTT hoặc bộ phận chuyên trách CNTT dự thảo Quyết định trình giảm đốc Sở TT&TT là giao nhiệm vụ là bộ phận chuyên trách về an toàn thông tin.

2.2. Phối hợp với những cơ quan/tổ chức có thẩm quyền

Yêu cầu	Có quy định về việc phối hợp với những cơ quan/tổ chức có thẩm quyền.
Phương án	Phối hợp với những cơ quan/tổ chức có thẩm quyền:

	1. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin: a) UBND tỉnh B giao Sở TT&TT là đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin tại Quyết định số .... b) Sở TT&TT làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng trên địa bàn tỉnh. c) Sở TT&TT chủ trì, phối hợp với Văn phòng Ủy ban nhân dân tỉnh, Công an tỉnh và các đơn vị có liên quan tiến hành kiểm tra công tác bảo đảm an toàn thông tin mạng định kỳ hàng năm hoặc theo chỉ đạo của UBND tỉnh đối với các cơ quan nhà nước trong tỉnh. 2. Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin: Tùy theo mức độ sự cố, phối hợp Cục An toàn thông tin hoặc Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam và các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố an toàn thông tin mạng

3. Bảo đảm nguồn nhân lực

3.1. Tuyển dụng

Yêu cầu	Có quy định về tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ.
Phương án	Quy định về tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ: 1. Quy định cán bộ được tuyển dụng vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng; 2. Xây dựng quy trình tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ.

3.2. Trong quá trình làm việc

Yêu cầu	Có quy định về việc thực hiện bảo đảm an toàn thông tin trong quá trình làm việc.
Phương án	Quy định về việc thực hiện bảo đảm an toàn thông tin trong quá trình làm việc: 1. Trách nhiệm bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống a) Với người sử dụng:

	- Người sử dụng có trách nhiệm đảm bảo ATTT đối với từng vị trí công việc. Trước khi tham gia vào hệ thống phải được kiểm tra khả năng đáp ứng các yêu cầu về ATTT. - Phải được thường xuyên tổ chức quán triệt các quy định về ATTT, nhằm nâng cao nhận thức về trách nhiệm đảm bảo ATTT. - Cá nhân, tổ chức phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp thiết bị b) Với cán bộ quản lý và vận hành hệ thống - Cán bộ chuyên trách phải thiết lập phương pháp hạn chế truy cập mạng không dây, giám sát và điều khiển truy cập không dây, tổ chức sử dụng chứng thực và mã hóa để bảo vệ truy cập không dây tới hệ thống thông tin. - Cán bộ chuyên trách phải tổ chức quản lý định danh đối với tất cả người dùng tham gia sử dụng hệ thống thông tin. 2. Định kỳ hàng năng người sử dụng được tổ chức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin theo chương trình, nội dung tại Quyết định số 893/QĐ-TTg ngày 19/6/2015 về việc phê duyệt Đề án Tuyên truyền, phổ biến, nâng cao nhận thức và trách nhiệm về an toàn thông tin đến năm 2020. 3. Định kỳ hàng năng người sử dụng được tổ chức đào tạo các kỹ năng cơ bản về an toàn thông tin theo chương trình, nội dung tại - Quyết định số 99/QĐ-TTg ngày 14/01/2014 phê duyệt Đề án Đào tạo và phát triển nguồn nhân lực an toàn, an ninh thông tin đến năm 2020.

3.3. Chấm dứt hoặc thay đổi công việc

Yêu cầu	Có quy định đối với cán bộ nghỉ hoặc thay đổi công việc.
Phương án	Quy định đối với cán bộ nghỉ hoặc thay đổi công việc: 1. Cán bộ nghỉ hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác thuộc sở hữu của tổ chứ. 2. Cán bộ quản trị phải vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc. 3. Cán bộ nghỉ hoặc thay đổi công việc phải có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc.

4. Quản lý thiết kế, xây dựng hệ thống thông tin

4.1. Thiết kế an toàn hệ thống thông tin

Yêu cầu	Có quy định về thiết kế an toàn hệ thống thông tin.
Phương án	Quy định đối với tài liệu thiết kế hệ thống: 1. Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin. 2. Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin. 3. Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin. 4. Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin. 5. Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống.

4.2. Phát triển phần mềm thuê khoán

Yêu cầu	Có quy định về phát triển phần mềm thuê khoán.
Phương án	Quy định đối với việc phát triển phần mềm thuê khoán: 1. Có điều khoản hợp đồng và các cam kết đối với bên thuê khoán khi thực hiện các nội dung liên quan đến việc phát triển phần mềm thuê khoán. 2. Các nhà phát triển cung cấp mã nguồn phần mềm. 3. Phần mềm thuê khoán phải được kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng. 4. Phần mềm thuê khoán phải được kiểm tra, đánh giá an toàn thông tin, trước khi đưa vào sử dụng.

4.3. Thử nghiệm và nghiệm thu hệ thống

Yêu cầu	Có quy định về việc thử nghiệm và nghiệm thu hệ thống.
Phương án	Quy định đối với việc thử nghiệm và nghiệm thu hệ thống: 1. Bên triển khai xây dựng kế hoạch, nội dung thử nghiệm hệ thống, trình cấp có thẩm quyền phê duyệt, trước khi thực hiện thử nghiệm và nghiệm thu hệ thống. 2. Hệ thống phải được thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng theo nội dung, kế hoạch được phê

	duyệt. 3. Có bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống. 4. Có đơn vị độc lập (bên thứ ba hoặc bộ phận độc lập thuộc đơn vị thực hiện tư vấn và giám sát quá trình thử nghiệm và nghiệm thu hệ thống. 5. Có báo cáo nghiệm thu được xác nhận của bộ phận chuyên trách và phê duyệt của chủ quản hệ thống thông tin trước khi đưa vào sử dụng.

5. Quản lý vận hành hệ thống thông tin

5.1. Quản lý an toàn mạng

Yêu cầu	Có quy định về quản lý an toàn mạng.
Phương án	Quy định về quản lý an toàn mạng: 1. Hệ thống mạng phải được thiết kế thống nhất, cùng kết hợp và hỗ trợ, tương tác hoạt động với nhau, được tổ chức quản lý định danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý hệ thống chặt chẽ, bảo đảm an toàn và bảo mật. 2. Hệ thống mạng phải được thiết lập cấu hình để: Kiểm soát truy cập từ bên ngoài mạng; Kiểm soát truy cập từ bên trong mạng; Kết nối về hệ thống giám sát tập trung; Phòng chống xâm nhập giữa các vùng mạng; Phòng chống phần mềm độc hại trên môi trường mạng. 3. Các thiết bị mạng phải được cấu hình chức năng xác thực; Chỉ cho phép sử dụng các kết nối mạng an toàn (nếu hỗ trợ) khi truy cập, quản trị thiết bị từ xa; Giới hạn các địa chỉ mạng có thể kết nối, quản trị thiết bị từ xa; Hạn chế được số lần đăng nhập sai; Phân quyền truy cập, quản trị; Nâng cấp, xử lý điểm yếu an toàn thông tin của thiết bị hệ thống trước khi đưa vào sử dụng. 4. Hệ thống mạng phải được trang bị hệ thống kỹ thuật, công nghệ hiện đại để thường xuyên, liên tục quản lý, giám sát, kiểm soát mạng nhằm phát hiện, ngăn chặn các truy cập trái phép của người sử dụng, tin tặc tấn công; triển khai cơ chế phòng chống vi rút tin học, thư rác cho những hệ thống xung yếu (máy chủ thư điện tử, máy chủ website, máy chủ tên miền, v.v...) và tại các máy chủ, máy trạm khác trong hệ thống.

	5. Việc thanh lý, tiêu hủy thiết bị, vật mang thông tin trong mạng Bộ phải đảm bảo yêu cầu không để lộ, lọt thông tin Nhà nước. Phải có quy trình cụ thể và phải lưu giữ hồ sơ, biên bản việc thanh lý, tiêu hủy. 6. Các yêu cầu đối với phòng máy chủ: a) Phòng máy chủ của các cơ quan là khu vực hạn chế tiếp cận và được được lắp đặt hệ thống camera giám sát. Chỉ những người có trách nhiệm theo quy định của Thủ trưởng cơ quan mới được phép vào phòng máy chủ. b) Phòng máy chủ phải có hệ thống lưu điện đủ công suất và duy trì thời gian hoạt động của các máy chủ tối thiểu 15 phút khi có sự cố mất điện. c) Bố trí cán bộ có năng lực chuyên môn cao để quản lý, vận hành phòng máy chủ và duy trì chế độ trực để đảm bảo an toàn thông tin mạng. 7. Đối với các thiết bị mạng chính a) Phải lắp đặt thiết bị chống sét để bảo vệ hệ thống CNTT, phải xây dựng ít nhất 02 thiết bị chống sét: một cho một đường cung cấp điện và một đường của mạng nội bộ (LAN). c) Thiết bị chuyển mạch (switch): Thiết bị chuyển mạch mạng tin học của các cơ quan phải đảm bảo khả năng cung cấp các chức năng quản trị nhằm tăng cường độ an toàn và bảo mật cho hệ thống mạng như: cung cấp khả năng từ chối các kết nối không mong muốn vào hệ thống trên từng cổng, quy định địa chỉ IP cho từng cổng và khống chế số lượng kết nối vào hệ thống mạng nội bộ thông qua thiết bị chuyển mạch. Phải có ít nhất 01 thiết bị chuyển mạch có hỗ trợ định tuyến IP (IP routing) cho mỗi mạng nội bộ, hỗ trợ chức năng điều khiển truy cập (Access Control List), hỗ trợ chức năng xác thực thiết bị và người sử dụng (User & Device Authentication) và chức năng bảo mật quản trị mạng (Network Administration Security). c) Tường lửa (firewall): Các cơ quan phải xây dựng tường lửa đảm bảo các yêu cầu gồm khả năng xử lý được số lượng kết nối đồng thời cao, hỗ trợ các công nghệ mạng riêng ảo thông dụng và có phần cứng mã hóa tích hợp để tăng tốc độ mã hóa dữ liệu, cung cấp đầy đủ các cơ chế bảo mật cơ bản như NAT, PAT, quản lý luồng dữ liệu

	vào, ra và có khả năng bảo vệ hệ thống trước các loại tấn công từ chối dịch vụ (DDoS). 8. Tệp tin cấu hình, sơ đồ mạng logic và vật lý phải được cập nhật, sao lưu dự phòng. 9. Có biện pháp bảo vệ, dự phòng, phòng chống các nguy cơ do mất cắp, cháy nổ, ngập lụt, động đất và các thảm họa khác do thiên nhiên hoặc con người gây ra và các phương án khôi phục hệ thống sau thảm họa.

5.2. Quản lý an toàn máy chủ và ứng dụng

Yêu cầu	Có quy định về quản lý an toàn máy chủ và ứng dụng.
Phương án	Quy định về quản lý an toàn máy chủ và ứng dụng: 1. Quy định với máy chủ a) Hệ thống máy chủ phải có tính năng sẵn sàng cao, cơ chế dự phòng linh hoạt để đảm bảo hoạt động liên tục. b) Có biện pháp bảo vệ, dự phòng, phòng chống các nguy cơ do mất cắp, cháy nổ, ngập lụt, động đất và các thảm họa khác do thiên nhiên hoặc con người gây ra và các phương án khôi phục sau thảm họa cho hệ thống máy chủ. c) Máy chủ phải được thiết lập chính sách xác thực; Kiểm soát truy cập; Kết nối về hệ thống giám sát tập trung; Thực hiện biện pháp phòng chống xâm nhập; Phòng chống phần mềm độc hại và xử lý dữ liệu trên máy chủ khi chuyển giao. d) Máy chủ phải được nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng. e) Việc kết nối, gỡ bỏ máy chủ khỏi hệ thống phải được sự cho phép của Thủ trưởng đơn vị và thực hiện theo quy trình đã được phê duyệt. g) Phần mềm hệ điều hành cài lên máy chủ ưu tiên là phần mềm hệ điều hành có bản quyền hoặc là phần mềm mã nguồn mở được sử dụng rộng rãi trong nước và quốc tế. h) Có tài liệu liệt kê, cài đặt với những phần mềm hệ thống cài trong máy chủ. 2. Quy định với ứng dụng:

	a) Các yêu cầu, thiết kế về an toàn bảo mật của phần mềm ứng dụng cần được xác định rõ trong tài liệu phân tích, thiết kế. Trong quá trình triển khai, vận hành các phần mềm ứng dụng cần đảm bảo nghiêm ngặt theo các yêu cầu, thiết kế về an toàn bảo mật. b) Ứng dụng phải được thiết lập chính sách xác thực; Kiểm soát truy cập; Kết nối về hệ thống giám sát tập trung; Có phương án bảo mật thông tin liên lạc, chống chối bỏ và biện pháp bảo đảm an toàn ứng dụng và mã nguồn. c) Có phương án xác định và khắc phục rủi ro trước, trong quá trình triển khai và khi vận hành các phần mềm ứng dụng. d) Ứng dụng phải kiểm tra, thử nghiệm và có biên bản đánh giá tính an toàn, bảo mật đối với phần mềm ứng dụng theo yêu cầu khi nghiệm thu các phần mềm này. Việc tiến hành thử nghiệm phải đảm bảo trên môi trường riêng biệt, không ảnh hưởng tới hoạt động và dữ liệu của đơn vị. 3. Quy định với ứng dụng thư điện tử: a) Không sử dụng các hộp thư điện tử công cộng. Không sử dụng thư điện tử chính thức của đơn vị vào mục đích cá nhân. b) Mỗi cá nhân cần đặt mật khẩu đủ mạnh cho hộp thư điện tử của mình. c) Đơn vị quản lý hệ thống thư điện tử cần có quy định về việc khóa và xóa bỏ hộp thư điện tử cá nhân khi cá nhân đó không còn làm việc tại đơn vị. d) Đơn vị quản lý hệ thống thư điện tử cần xây dựng phương án đảm bảo an toàn và tính khả dụng truy cập cho hệ thống thư điện tử trong nội bộ và trên Internet, phương án chống thư rác cho thư điện tử. 4. Quy định đối với cổng/trang thông tin điện tử a) Quản lý toàn bộ các phiên bản của mã nguồn, phối hợp với đơn vị thực hiện dịch vụ hosting tổ chức mô hình trang web hợp lý, tránh khả năng tấn công leo thang đặc quyền. Yêu cầu đơn vị cung cấp dịch vụ hosting phải cài đặt các hệ thống phòng vệ như tường lửa thiết bị phát hiện/phòng chống xâm nhập (IDS/IPS) ở mức ứng dụng web (WAF- Web Application Firewall). b) Các trang web khi đưa vào sử dụng hoặc khi bổ sung thêm các chức năng, dịch vụ công mới cần đánh giá kiểm định nhằm tránh

	được các lỗi bảo mật thường xảy ra trên ứng dụng web như: SQL Injection, Cross-Site Scripting (xss), ... c) Phối hợp với các nhà cung cấp dịch vụ hosting xây dựng phương án phục hồi trang web, trong đó chú ý mỗi tháng thực hiện việc backup toàn bộ nội dung trang web một lần bao gồm mã nguồn, cơ sở dữ liệu, dữ liệu phi cấu trúc... để bảo đảm khi có sự cố có thể khắc phục lại ngay trong vòng 24 giờ. d) Bảo đảm an toàn cho Cổng/Trang thông tin điện tử: Thực hiện theo hướng dẫn tại công văn số 2132/BTTTT-VNCERT ngày 18 tháng 7 năm 2011 của Bộ về việc hướng dẫn đảm bảo an toàn thông tin cho các Cổng/Trang thông tin điện tử.

5.3. Quản lý an toàn dữ liệu

Yêu cầu	Có quy định về quản lý an toàn dữ liệu.
Phương án	Quy định về quản lý an toàn dữ liệu: 1. Thực hiện quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã kiểm tra tính nguyên vẹn. 2. Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ. 3. Lưu trữ có mã hóa các thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trên hệ thống lưu trữ/phương tiện lưu trữ.

5.4. Quản lý an toàn thiết bị đầu cuối

Yêu cầu	Có quy định về quản lý thiết bị đầu cuối.
Phương án	Quy định về quản lý an toàn thiết bị đầu cuối: a) Thông tin về thiết bị đầu cuối (tên, chủng loại, địa chỉ MAC, địa chỉ IP) phải được quản lý và cập nhật. b) Các thiết bị đầu cuối phải được quản lý khi kết nối vào hệ thống mạng theo địa chỉ MAC, IP. c) Khi truy cập và sử dụng thiết bị đầu cuối từ xa phải có cơ chế xác thực và sử dụng giao thức mạng an toàn. c) Việc cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống phải được cho phép bởi người có thẩm quyền và thực hiện theo quy trình được phê duyệt.

5.5. Quản lý phòng chống phần mềm độc hại

Yêu cầu	Có quy định về quản lý phòng chống phần mềm độc hại.
Phương án	Quy định về quản lý phòng chống phần mềm độc hại: 1. Tất cả các máy trạm, máy chủ phải được trang bị phần mềm phòng chống mã độc. Các phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc khi sao chép, mở các tập tin. 2. Khi gửi văn bản điện tử gửi qua hệ thống thư điện tử phải có định dạng theo Danh mục tiêu chuẩn kỹ thuật về ứng dụng CNTT trong cơ quan nhà nước như: (.txt), (.doc), (.odt), (.pdf) và các định dạng khác theo quy định, không được gửi các file thực thi (.com), (.bat), (.exe) …. 3. Các cán bộ, công chức, viên chức và người lao động trong cơ quan phải được hướng dẫn về phòng chống mã độc, các rủi ro do mã độc gây ra; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm trên máy trạm khi chưa có sự đồng ý của người có thẩm quyền theo quy định của cơ quan. 4. Tất cả các máy tính của đơn vị phải được cấu hình nhằm vô hiệu hóa tính năng tự động thực thi (autoplay) các tập tin trên các thiết bị lưu trữ di động. 5. Khi phát hiện ra bất kỳ dấu hiện nào liên quan đến việc bị nhiễm mã độc trên máy trạm (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu…), người sử dụng phải báo trực tiếp cho bộ phận có trách nhiệm của đơn vị để xử lý. 6. Phần mềm ứng dụng trước khi được cài đặt, sử dụng phải được kiểm tra xem có phần mềm độc hại tồn tại hay không? Tất cả các tập tin, thư mục phải được quét mã độc trước khi sao chép, sử dụng. 7. Định kỳ hàng năm thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; Thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống.

5.6. Quản lý giám sát an toàn hệ thống thông tin

Yêu cầu	Có quy định về quản lý giám sát an toàn hệ thống thông tin.
Phương án	Quy định về quản lý giám sát an toàn hệ thống thông tin:

	1. Triển khai hệ thống giám sát trung tâm phải đáp ứng yêu cầu tại khoản 1, Điều 5 Thông tư số 31/2017/TT-BTTTT. 2. Thông tin giám sát và danh mục các đối tượng giám sát phải đáp ứng yêu cầu tại khoản 2, Điều 5 Thông tư số 31/2017/TT-BTTTT. Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát. 3. Thực thi nhiệm vụ giám sát theo quy định tại khoản 3, Điều 5 Thông tư số 31/2017/TT-BTTTT. 4. Định kỳ hàng năm tổ chức nâng cao năng lực hoạt động giám sát theo quy định tại Điều 9 Thông tư số 31/2017/TT-BTTTT. 5. Chủ quản hệ thống thông tin có trách nhiệm giám sát an toàn thông tin theo quy định tại Điều 14 Thông tư số 31/2017/TT-BTTTT.

5.7. Quản lý điểm yếu an toàn thông tin

Yêu cầu	Có quy định về quản lý điểm yếu an toàn thông tin.
Phương án	Quy định về quản lý điểm yếu an toàn thông tin: 1. Đơn vị/bộ phận chuyên trách về an toàn thông tin có trách nhiệm: a) Quản lý thông tin điểm yếu an toàn thông tin đối với từng thành phần có trong hệ thống (hệ điều hành, máy chủ, ứng dụng, dịch vụ…); Phân loại mức độ nguy hiểm của điểm yếu; Xây dựng phương án và quy trình xử lý đối với từng mức độ nguy hiểm của điểm yếu. b) Báo cáo Lãnh đạo/Cán bộ quản lý ngay khi phát hiện điểm yếu an toàn thông tin ở mức độ nghiêm trọng. Thực hiện cảnh báo và xử lý điểm yếu an toàn thông tin theo chỉ đạo. Việc xử lý điểm yếu an toàn thông tin phải bảo đảm không giám ảnh hưởng/gián đoạn hoạt động của hệ thống. c) Xây dựng phương án xử lý tạm thời đối với trường hợp điểm yếu an toàn thông tin chưa được khắc phục và phương án khôi phục hệ thống trong trường hợp xử lý điểm yếu thất bại. d) Có trách nhiệm phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu an toàn thông tin đối với các điểm yếu khi cần thiết. 2. Đối với hệ thống/hệ thống thành phần được đề xuất là cấp độ 3

	trở lên phải thực hiện kiểm tra, đánh giá và xử lý điểm yếu an toàn thông tin cho thiết bị hệ thống, máy chủ, dịch vụ trước khi đưa vào sử dụng. 3. Định kỳ hàng năm kiểm tra, đánh giá điểm yếu an toàn thông tin cho toàn bộ hệ thống thông tin; Thực hiện quy trình kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin khi có thông tin hoặc nhận được cảnh báo về điểm yếu an toàn thông tin đối với thành phần cụ thể trong hệ thống. 4. Hoạt động đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thực hiện theo quy định tại điểm c khoản 2 Điều 20 Nghị định số 85/2016/NĐ-CP và Điều 13 Thông tư số 03/2017/TT-BTTTT

5.8. Quản lý sự cố an toàn thông tin

Yêu cầu	Có quy định về quản lý sự cố an toàn thông tin.
Phương án	Quy định về quản lý sự cố an toàn thông tin: 1. Đơn vị/bộ phận chuyên trách về an toàn thông tin có trách nhiệm: a) Phân nhóm sự cố an toàn thông tin mạng theo quy định tại Quyết định số 05/2017/NĐ-CP của Thủ tướng Chính phủ ngày 16/3/2017 quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia (Quyết định 05); Xây dựng phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng, ứng phó sự cố an toàn thông tin mạng. b) Xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13,14 Quyết định số 05. c) Xây dựng và triển khai kế hoạch ứng phó sự cố an toàn thông tin theo quy định tại Điều 16 Quyết định số 05. d) Quyết định toàn diện về mặt kỹ thuật đối với các cơ quan trong quá trình khắc phục sự cố về ATTT; Hỗ trợ, phối hợp và hướng dẫn các cơ quan khắc phục sự cố mất ATTT; Yêu cầu ngưng hoạt động một phần hoặc toàn bộ các hệ thống thông tin của các cơ quan nhằm phục vụ công tác khắc phục sự cố về ATTT; Phối hợp với đơn vị chức năng trong điều tra các nguyên nhân gây ra sự cố mất an toàn thông tin theo chỉ đạo của Lãnh đạo. e) Phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin;

	Yêu cầu bên cung cấp, hỗ trợ cung cấp quy trình xử lý sự cố cho các dịch vụ do bên cung cấp, hỗ trợ cung cấp liên quan đến hệ thống. g) Tổ chức diễn tập phương án xử lý sự cố an toàn thông tin theo chỉ đạo của Lãnh đạo. 2. Trách nhiệm của người dùng: Thông tin, báo cáo kịp thời cho cán bộ chuyên trách về ATTT của cơ quan khi phát hiện các sự cố gây mất ATTT trong quá trình tham gia vào hệ thống thông tin của đơn vị; Phối hợp tích cực trong suốt quá trình giải quyết và khắc phục sự cố.

5.9. Quản lý an toàn người sử dụng đầu cuối

Yêu cầu	Có quy định về quản lý an toàn người sử dụng đầu cuối.
Phương án	Quy định về quản lý an toàn người sử dụng đầu cuối: 1. Kết nối máy tính/thiết bị đầu cuối của người sử dụng vào hệ thống: a) Người sử dụng khi truy cập, sử dụng tài nguyên nội bộ, truy cập mạng và tài nguyên trên Internet phải tuân thủ các quy định của pháp luật về bảo đảm an toàn thông tin và các quy định của cơ quan, tổ chức. b) Khi cài đặt, kết nối máy tính/thiết bị đầu cuối phải thực hiện theo hướng dẫn/quy trình dưới sự giám sát của bộ phận chuyên trách về an toàn thông tin. c) Đối với hệ thống thông tin có cấp độ 3 trở lên, máy tính/thiết bị đầu cuối phải được xử lý điểm yếu an toàn thông tin, cấu hình cứng hóa bảo mật trước khi kết nối vào hệ thống. 2. Trong quá trình sử dụng: a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao; b) Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng; c) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách công nghệ thông tin của cơ quan, đơn vị để kịp thời ngăn chặn và xử lý; d) Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng được tỉnh hoặc đơn vị chuyên môn tổ chức.

II. Thuyết minh phương án đáp ứng yêu cầu kỹ thuật

1. Bảo đảm an toàn mạng

1.1. Thiết kế hệ thống

- Các vùng mạng trong hệ thống:

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Vùng mạng biên	Có	Kết nối hệ thống với mạng Internet và mạng diện rộng
2	Vùng DMZ	Có	Vùng máy chủ dịch vụ, cung cấp dịch vụ trực tiếp ra bên ngoài Internet
3	Vùng máy chủ nội bộ	Có	Vùng máy chủ nội bộ, cung cấp các dịch vụ nội bộ
4	Vùng mạng máy chủ CSDL	Có	Vùng mạng cho các máy chủ cơ sở dữ liệu để quản lý và bảo vệ tập trung các máy chủ CSDL.
5	Vùng quản trị	Có	Vùng mạng cho các máy tính quản trị và các máy chủ hệ thống.

- Phương án bảo đảm an toàn thông tin

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Phương án quản lý truy cập, quản trị hệ thống từ xa an toàn	Có	Các thiết bị hệ thống/máy chủ được thiết lập cấu hình cho phép quản trị từ xa an toàn.
2	Phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập	Có	Truy cập giữa các vùng mạng được quản lý và phòng chống xâm nhập sử dụng các thiết bị tường lửa chuyên dụng có tích hợp chức năng phòng chống xâm nhập.
3	Phương án cân bằng tải và dự phòng nóng cho các thiết bị mạng chính	Có	Các thiết bị mạng chính được thiết kế và cấu hình hoạt động ở chế độ A-A (Thiết kế chi tiết tại Sơ đồ vật lý và logic gửi kèm theo).
4	Phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu	Chưa có	Chưa có phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu. Sẽ xây dựng phương án bổ sung (Thực hiện trước 12/2018)
5	Phương án chặn lọc phần mềm độc hại trên môi trường mạng	Chưa có	Chưa có chặn lọc phần mềm độc hại trên môi trường mạng. Sẽ xây dựng phương án bổ sung (Thực hiện trước 12/2018)

6	Phương án phòng chống tấn công từ chối dịch vụ	Có	Hệ thống sử dụng giải pháp của hãng Abor được triển khai ở vùng mạng biên để thực hiện phát hiện và phòng chống tấn công DoS/DDoS
7	Phương án giám sát hệ thống thông tin tập trung	Có	Hệ thống sử dụng giải pháp HP OpenView/Solarwinds/Cacti/Nagios/MRTG để thực hiện giám sát hoạt động của hệ thống mạng, bảo đảm tính khả dụng của hệ thống.
8	Phương án giám sát an toàn hệ thống thông tin tập trung	Có	Hệ thống sử dụng giải pháp ArcSight/Splunk/QRadar/LogRhythm được triển khai ở vùng mạng quản trị, cho phép quản trị tập trung nhật ký hệ thống từ các thiết bị/máy chủ
9	Phương án quản lý sao lưu dự phòng tập trung	Có	Sử dụng hệ thống SAN của hãng HP, có năng lực quản lý và lưu trữ 20T dữ liệu.
10	Có phương án quản lý phần mềm phòng chống mã độc trên các máy chủ/máy tính người dùng tập trung	Chưa có	Chưa có phương án quản lý phần mềm phòng chống mã độc trên các máy chủ/máy tính người dùng tập trung. Sẽ bổ phương án và giải pháp (Thực hiện trước 12/2018).
11	Có phương án phòng, chống thất thoát dữ liệu	Chưa có	Chưa có phương án phòng, chống thất thoát dữ liệu. Sẽ bổ phương án và giải pháp (Thực hiện trước 12/2018).
12	Có phương án dự phòng kết nối mạng Internet cho hệ thống	Có	Sử dụng đồng thời hai kết nối Internet của hai nhà cung cấp dịch vụ khác nhau.

1.2. Kiểm soát truy cập từ bên ngoài mạng

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập thông tin nội bộ hoặc quản trị hệ thống từ các mạng bên ngoài và mạng Internet	Có	Hệ thống được thiết lập chỉ cho phép kết nối mạng có hỗ trợ mã hóa, xác thực khi truy cập thông tin nội bộ hoặc quản trị hệ thống từ các mạng bên ngoài và mạng Internet.
2	Kiểm soát truy cập từ bên	Có	Hệ thống được thiết lập chỉ cho phép

	ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể; chặn tất cả truy cập tới các dịch vụ, ứng dụng mà hệ thống không cung cấp hoặc không cho phép truy cập từ bên ngoài		kiểm soát truy cập từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể. Chính sách được thiết lập trên Fireall01 theo chiều từ bên ngoài vào vùng DMZ; trên Fireall03 theo chiều từ bên ngoài vào vùng quản trị; trên Fireall04 theo chiều từ bên ngoài vào vùng máy chủ nội bộ.
3	Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi hệ thống không nhận được yêu cầu từ người dùng.	Có	Thiết lập giới hạn thời gian chờ để đóng phiên kết nối khi hệ thống không nhận được yêu cầu từ người dùng được thiết lập trên các Firewall01, 02, 03, 04.
4	Phân quyền và cấp quyền truy cập từ bên ngoài vào hệ thống theo từng người dùng hoặc nhóm người dùng căn cứ theo yêu cầu nghiệp vụ, yêu cầu quản lý.	Có	Thực hiện chính sách trên thiết bị VPN Gateway tại vùng mạng biên. Mỗi người sử dụng sẽ có tài khoản khác nhau, khi kết nối VPN sẽ nhận được địa chỉ IP và chính sách truy cập vào hệ thống khác nhau.
5	Giới hạn số lượng kết nối đồng thời từ một địa chỉ nguồn và tổng số lượng kết nối đồng thời cho từng ứng dụng, dịch vụ được hệ thống cung cấp theo năng lực thực tế của hệ thống	Có	Giới hạn số lượng kết nối đồng thời từ một địa chỉ nguồn và tổng số lượng kết nối đồng thời cho từng ứng dụng, dịch vụ được thiết lập trên các Firewall01, 02, 03, 04.

1.3. Kiểm soát truy cập từ bên trong mạng

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Chỉ cho phép truy cập các ứng dụng, dịch vụ bên ngoài theo yêu cầu nghiệp vụ, chặn các dịch vụ khác không phục vụ hoạt động nghiệp vụ theo chính sách của tổ chức	Có	Người sử dụng chỉ được truy cập, sử dụng các dịch vụ sau từ các mạng bên ngoài để phục vụ hoạt động nghiệp vụ. Chính sách truy cập được thiết lập trên Firewall02.
2	Giới hạn truy cập các ứng	Có	Người sử dụng chỉ được truy ra bên

	dụng, dịch vụ bên ngoài theo thời gian		ngoài theo giờ hành chính vào các ngày trong tuần. Chính sách truy cập được thiết lập trên Firewall02.
3	Có phương án kiểm soát truy cập của người dùng vào các dịch vụ, các máy chủ nội bộ theo chức năng và chính sách của tổ chức	Có	Người sử dụng trong mạng được phân thành các Vlan khác nhau. Căn cứ vào địa chỉ của mỗi Vlan, chính sách truy cập vào từng máy chủ trong mạng nội bộ được thiết lập trên Firewall04.

1.4. Nhật ký hệ thống

Yêu cầu **Thiết bị**	Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên các thiết bị hệ thống	Sử dụng máy chủ thời gian trong hệ thống để đồng bộ thời gian	Lưu trữ và quản lý tập trung nhật ký hệ thống	Lưu trữ nhật ký hệ thống của thiết bị tối thiểu 03 tháng
Firewall01	+	+	+	+
Firewall01	+	+	+	-
CoreSw01	+	+	-	-
CoreSw02	+	+	-	-
DB APP Firewall	+	+	-	-
Anti-Spam	+	+	+	-

1.5. Phòng chống xâm nhập

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Có phương án phòng chống xâm nhập để bảo vệ các vùng mạng trong hệ thống	Có	Các vùng mạng được triển khai hệ thống IDS/IPS, hoạt động ở chế độ Inline cho phép phát hiện và phòng chống xâm nhập.
2	Định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng	Có	Đã thiết lập chức năng tự động cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng đều được thiết lập trên các thiết bị IDS/IPS.
3	Bảo đảm năng lực hệ thống đáp ứng đủ theo yêu cầu, quy mô số lượng người	Có	Các IDS/IPS có năng lực xử lý đáp ứng đủ theo yêu cầu, quy mô số lượng người dùng và dịch vụ, ứng dụng của hệ thống

	dùng và dịch vụ, ứng dụng của hệ thống cung cấp		cung cấp.

1.6. Phòng chống phần mềm độc hại trên môi trường mạng

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Có phương án phòng chống phần mềm độc hại trên môi trường mạng	Có	Chức năng phòng chống phần mềm độc hại trên môi trường mạng được tích hợp trên các Firewall. Các Firewall được thiết lập cấu hình để có thể phát hiện ra các hành vi mã độc trên môi trường mạng.
2	Định kỳ cập nhật dữ liệu cho hệ thống phòng chống phần mềm độc hại	Có	Đã thiết lập chức năng cập nhật dữ liệu cho hệ thống phòng chống phần mềm độc hại trên các Firewall có tích hợp chức năng phòng chống phần mềm độc hại trên môi trường mạng.
3	Bảo đảm năng lực hệ thống đáp ứng đủ theo yêu cầu, quy mô số lượng người dùng và dịch vụ, ứng dụng của hệ thống cung cấp	Có	Các các Firewall có tích hợp chức năng phòng chống phần mềm độc hại trên môi trường mạng có năng lực xử lý đáp ứng đủ theo yêu cầu, quy mô số lượng người dùng và dịch vụ, ứng dụng của hệ thống cung cấp.

1.8. Bảo vệ thiết bị hệ thống

Yêu cầu **Thiết bị**	Cấu hình chức năng xác thực trên các thiết bị	Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị thiết bị từ xa	Hạn chế các địa chỉ mạng có thể kết nối, quản trị thiết bị từ xa	Hạn chế được số lần đăng nhập sai	Phân quyền truy cập, quản trị thiết bị	Nâng cấp, xử lý điểm yếu an toàn thông tin của thiết bị hệ thống trước khi đưa vào sử dụng
Firewall01	+	+	+	+	+	+
Firewall01	+	+	+	+	+	+
CoreSw01	+	+	-	-	-	-
CoreSw02	+	+	-	-	-	+

DB APP Firewall	+	+	-	-	-	+
Anti-Spam	+	+	+	+	-	-

2. Bảo đảm an toàn máy chủ

2.1. Xác thực

Yêu cầu **Máy chủ**	Thiết lập chính sách xác thực trên máy chủ	Thay đổi các tài khoản mặc định trên hệ thống hoặc vô hiệu hóa	Thiết lập chính sách mật khẩu an toàn	Hạn chế số lần đăng nhập sai	vô hiệu hóa tài khoản nếu tài khoản đó đăng nhập sai nhiều lần vượt số lần quy định
Server01	+	+	+	+	+
Server02	+	+	+	-	+
Server03	+	+	-	-	-
Server04	+	+	-	-	+
Server05	+	+	-	-	-

2.2. Kiểm soát truy cập

Yêu cầu **Máy chủ**	Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa	Thiết lập giới hạn thời gian chờ (timeout)	Thay đổi cổng quản trị mặc định của máy chủ	Giới hạn địa chỉ mạng được phép truy cập, quản trị máy chủ từ xa
Server01	+	+	+	+
Server02	+	+	+	-
Server03	+	+	-	-
Server04	+	+	-	-
Server05	+	+	-	-

2.3. Nhật ký hệ thống

Yêu cầu / Máy chủ	Thiết lập lập chức năng ghi nhật ký hệ thống trên các máy chủ	Đồng bộ thời gian giữa máy chủ với máy chủ thời gian	Giới hạn đủ dung lượng lưu trữ nhật ký hệ thống để không mất hoặc tràn nhật ký hệ thống	Quản lý và lưu trữ tập trung nhật ký hệ thống thu thập được từ máy chủ	Lưu nhật ký hệ thống trong khoảng thời gian tối thiểu là 03 tháng
Server01	+	+	+	+	+
Server02	+	+	+	-	+
Server03	+	+	-	-	-
Server04	+	+	-	-	+
Server05	+	+	-	-	-

2.4. Phòng chống xâm nhập

Yêu cầu / Máy chủ	Loại bỏ các tài khoản không sử dụng, các tài khoản không còn hợp lệ trên máy chủ	Sử dụng tường lửa của hệ điều hành và hệ thống để cấm các truy cập trái phép tới máy chủ	Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ hệ thống không sử dụng	Thực hiện nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng
Server01	+	+	+	+
Server02	+	+	+	-
Server03	+	+	-	-
Server04	+	+	-	-
Server05	+	+	-	-

2.5. Phòng chống phần mềm độc hại

Yêu cầu / Máy chủ	Cài đặt phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật	Kiểm tra, dò quét, xử lý phần mềm độc hại cho các phần mềm trước khi cài đặt	Quản lý tập trung các phần mềm phòng chống mã độc cài đặt trên máy chủ
Server01	+	+	-
Server02	+	+	-
Server03	+	+	-
Server04	+	+	-
Server05	+	+	-

2.6. Xử lý máy chủ khi chuyển giao

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Có phương án xóa sạch thông tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng	Chưa có	Chưa có phương án xử lý máy chủ khi chuyển giao đáp ứng yêu cầu. Sẽ bổ sung phương án, sử dụng giải pháp công nghệ để đáp ứng yêu cầu. Dự kiến thực hiện trước tháng 12/2018.
2	Sao lưu dự phòng thông tin, dữ liệu trên máy chủ, bản dự phòng hệ điều hành máy chủ trước khi thực hiện xóa dữ liệu, hệ điều hành	Chưa có	
3	Có biện pháp kiểm tra, bảo đảm dữ liệu không thể khôi phục sau khi xóa	Chưa có	

3. Bảo đảm an toàn ứng dụng

3.1. Xác thực

Yêu cầu **Ứng dụng**	Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng	Lưu trữ có mã hóa thông tin xác thực hệ thống	Thiết lập cấu hình ứng dụng để đảm bảo an toàn mật khẩu người sử dụng	Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định	Mã hóa thông tin xác thực trước khi gửi qua môi trường mạng	Thiết lập cấu hình ứng dụng để ngăn cản việc đăng nhập tự động đối với các ứng dụng
Thư điện tử	+	+	+	+	+	-

3.2. Kiểm soát truy cập

Yêu cầu	Chỉ cho phép sử dụng các kết nối mạng an	Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên	Giới hạn địa chỉ mạng quản trị được phép truy cập,	Phân quyền truy cập, quản trị, sử dụng tài nguyên khác	Giới hạn số lượng các kết nối đồng thời (kết nối

Ứng dụng	toàn khi truy cập, quản trị ứng dụng từ xa	kết nối khi ứng dụng không nhận được yêu cầu từ người dùng	quản trị ứng dụng từ xa	nhau của ứng dụng với từng người/nhóm sử dụng	khởi tạo và đã thiết lập) đối với các ứng dụng
Thư điện tử	+	+	+	+	+

3.3. Nhật ký hệ thống

Yêu cầu	Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau: (1) Thông tin truy cập ứng dụng (2) Thông tin đăng nhập khi quản trị ứng dụng; (3) Thông tin các lỗi phát sinh trong quá trình hoạt động (4) Thông tin thay đổi cấu hình ứng dụng	Quản lý và lưu trữ nhật ký hệ thống trên hệ thống quản lý tập trung	Nhật ký hệ thống phải được lưu trữ trong khoảng thời gian tối thiểu là 03 tháng
Ứng dụng			
Thư điện tử	+	+	+

3.4. Bảo mật thông tin liên lạc

Yêu cầu	Mã hóa thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trước khi truyền đưa, trao đổi qua môi trường mạng; sử dụng phương án mã hóa theo quy định về bảo vệ bí mật nhà nước đối với thông tin mật.	Sử dụng kết nối mạng an toàn, bảo đảm an toàn trong quá trình khởi tạo kết nối kênh truyền và trao đổi thông tin qua kênh truyền
Ứng dụng		
Thư điện tử	+	+

3.5. Chống chối bỏ

Yêu cầu	Sử dụng chữ ký số khi trao đổi thông tin, dữ liệu quan trọng
Ứng dụng	
Thư điện tử	+

3.6. An toàn ứng dụng và mã nguồn

Yêu cầu **Ứng dụng**	Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý	Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu ra trước khi gửi về máy yêu cầu	Giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị ứng dụng từ xa	Có phương án bảo vệ ứng dụng chống lại những dạng tấn công phổ biến: SQL Injection, OS command injection, RFI, LFI, Xpath injection, XSS, CSRF
Thư điện tử	+	+	+	-

4. Bảo đảm an toàn dữ liệu

4.1. Nguyên vẹn dữ liệu

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Có phương án quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã kiểm tra tính nguyên vẹn	Có	Dữ liệu quan trọng trên hệ thống bao gồm dữ liệu: dữ liệu nghiệp vụ, văn bản điện tử quan trọng và dữ liệu cấu hình hệ thống. Dữ liệu được nén và được lưu trữ cùng mã kiểm tra MD5 trên hệ thống SAN.

4.2. Bảo mật dữ liệu

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Lưu trữ có mã hóa các thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trên hệ thống lưu trữ/phương tiện lưu trữ	Có	Dữ liệu quan trọng trên hệ thống bao gồm dữ liệu: dữ liệu nghiệp vụ, văn bản điện tử quan trọng và dữ liệu cấu hình hệ thống. Dữ liệu được nén và được lưu trữ mã hóa sử dụng công cụ XXX (hỗ trợ các chuẩn mã hóa: DES, AES…) trên hệ thống SAN.

4.3. Sao lưu dự phòng

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Thực hiện sao lưu dự phòng các thông tin, dữ liệu cơ bản sau: tập	Có	Thông tin, dữ liệu được lưu trữ và quản lý tập trung trên

	tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ		hệ thống lưu trữ SAN.
2	Phân loại và quản lý các dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau	Có	Thông tin dữ liệu được phân theo từng nhóm theo đặc trưng nghiệp vụ hoặc chức năng. Được quy định về việc đặt tên các tập tin/thư mục khi lưu trữ trên hệ thống.
3	Có hệ thống/phương tiện lưu trữ độc lập để sao lưu dự phòng	Có	Hệ thống SAN được phân vùng lưu trữ riêng để phục vụ việc lưu trữ thông tin, dữ liệu.

PHỤ LỤC III
QUY CHẾ BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. Phạm vi điều chỉnh:

Quy chế này quy định các chính sách quản lý và các biện pháp nhằm bảo đảm an toàn thông tin các hệ thống thông tin trên địa bàn tỉnh.

2. Đối tượng áp dụng:

a) Cơ quan hành chính, đơn vị sự nghiệp, doanh nghiệp thuộc UBND; Cán bộ thuộc các đơn vị thuộc UBND.

b) Cơ quan, tổ chức, cá nhân có kết nối vào mạng máy tính trong phạm vi toàn Tỉnh .

c) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ công nghệ thông tin và an toàn thông tin mạng cho các đơn vị thuộc UBND.

Điều 2. Giải thích từ ngữ

Trong quy chế này, các từ ngữ dưới đây được hiểu như sau:

1. *An toàn thông tin mạng* là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

2. *Mạng* là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua mạng viễn thông và mạng máy tính.

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

4. *Hệ thống thông tin quan trọng quốc gia* là hệ thống thông tin mà khi bị phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới quốc phòng, an ninh quốc gia.

5. *Chủ quản hệ thống thông tin* là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin.

6. *Xâm phạm an toàn thông tin mạng* là hành vi truy nhập, sử dụng, tiết lộ, làm gián đoạn, sửa đổi, phá hoại trái phép thông tin, hệ thống thông tin.

7. *Sự cố an toàn thông tin mạng* là việc thông tin, hệ thống thông tin bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.

8. *Rủi ro an toàn thông tin mạng* là những nhân tố chủ quan hoặc khách quan có khả năng ảnh hưởng tới trạng thái an toàn thông tin mạng.

9. *Đánh giá rủi ro an toàn thông tin mạng* là việc phát hiện, phân tích, ước lượng mức độ tổn hại, mối đe dọa đối với thông tin, hệ thống thông tin.

10. *Quản lý rủi ro an toàn thông tin mạng* là việc đưa ra các biện pháp nhằm giảm thiểu rủi ro an toàn thông tin mạng.

11. *Phần mềm độc hại* là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

12. *Hệ thống lọc phần mềm độc hại* là tập hợp phần cứng, phần mềm được kết nối vào mạng để phát hiện, ngăn chặn, lọc và thống kê phần mềm độc hại.

13. *Địa chỉ điện tử* là địa chỉ được sử dụng để gửi, nhận thông tin trên mạng bao gồm địa chỉ thư điện tử, số điện thoại, địa chỉ Internet và hình thức tương tự khác.

14. *Xung đột thông tin* là việc hai hoặc nhiều tổ chức trong nước và nước ngoài sử dụng biện pháp công nghệ, kỹ thuật thông tin gây tổn hại đến thông tin, hệ thống thông tin trên mạng.

15. *Thông tin cá nhân* là thông tin gắn với việc xác định danh tính của một người cụ thể.

16. *Chủ thể thông tin cá nhân* là người được xác định từ thông tin cá nhân đó.

17. *Xử lý thông tin cá nhân* là việc thực hiện một hoặc một số thao tác thu thập, biên tập, sử dụng, lưu trữ, cung cấp, chia sẻ, phát tán thông tin cá nhân trên mạng nhằm mục đích thương mại.

18. *Mật mã dân sự* là kỹ thuật mật mã và sản phẩm mật mã được sử dụng để bảo mật hoặc xác thực đối với thông tin không thuộc phạm vi bí mật nhà nước.

19. *Sản phẩm an toàn thông tin mạng* là phần cứng, phần mềm có chức năng bảo vệ thông tin, hệ thống thông tin.

20. *Dịch vụ an toàn thông tin mạng* là dịch vụ bảo vệ thông tin, hệ thống thông tin.

Điều 3. Nguyên tắc bảo đảm an toàn thông tin

1. Cơ quan, tổ chức, cá nhân có trách nhiệm bảo đảm an toàn thông tin mạng. Hoạt động an toàn thông tin mạng của cơ quan, tổ chức, cá nhân phải đúng quy

định của pháp luật, bảo đảm quốc phòng, an ninh quốc gia, bí mật nhà nước, giữ vững ổn định chính trị, trật tự, an toàn xã hội và thúc đẩy phát triển kinh tế - xã hội.

2. Tổ chức, cá nhân không được xâm phạm an toàn thông tin mạng của tổ chức, cá nhân khác.

3. Việc xử lý sự cố an toàn thông tin mạng phải bảo đảm quyền và lợi ích hợp pháp của tổ chức, cá nhân, không xâm phạm đến đời sống riêng tư, bí mật cá nhân, bí mật gia đình của cá nhân, thông tin riêng của tổ chức.

4. Hoạt động an toàn thông tin mạng phải được thực hiện thường xuyên, liên tục, kịp thời và hiệu quả.

Điều 4. Những hành vi nghiêm cấm

1. Các hành vi bị nghiêm cấm quy định tại Điều 7 Luật An toàn thông tin mạng.

2. Tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập không dây của cá nhân vào mạng nội bộ; trên cùng một thiết bị thực hiện đồng thời truy cập vào mạng nội bộ và truy cập Internet bằng thiết bị kết nối Internet của cá nhân (modem quay số, USB 3G/4G, điện thoại di động, máy tính bảng, máy tính xách tay).

3. Tự ý thay đổi, gỡ bỏ biện pháp an toàn thông tin cài đặt trên thiết bị công nghệ thông tin phục vụ công việc; tự ý thay thế, lắp mới, tráo đổi thành phần của máy tính phục vụ công việc.

Điều 5. Phối hợp với những cơ quan/tổ chức có thẩm quyền

1. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin:

a) UBND tỉnh A giao Sở TT&TT là đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin tại Quyết định số...

b) Sở TT&TT làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng trên địa bàn tỉnh.

c) Sở TT&TT chủ trì, phối hợp với Văn phòng Ủy ban nhân dân tỉnh, Công an tỉnh và các đơn vị có liên quan tiến hành kiểm tra công tác bảo đảm an toàn thông tin mạng định kỳ hàng năm hoặc theo chỉ đạo của UBND tỉnh đối với các cơ quan nhà nước trong tỉnh.

2. Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin: Tùy theo mức độ sự cố, phối hợp Cục An toàn thông tin hoặc Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam và các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố an toàn thông tin mạng

Điều 6. Bảo đảm nguồn nhân lực

1. Xây dựng các quy định đối với công tác tuyển dụng

a) Yêu cầu các cán bộ được tuyển dụng vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng;

b) Yêu cầu xây dựng các quy trình tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ.

2. Xây dựng các quy định về việc thực hiện bảo đảm an toàn thông tin trong quá trình làm việc:

a) Trách nhiệm bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống

i) Với người sử dụng:

- Người sử dụng có trách nhiệm đảm bảo ATTT đối với từng vị trí công việc. Trước khi tham gia vào hệ thống phải được kiểm tra khả năng đáp ứng các yêu cầu về ATTT.

- Phải được thường xuyên tổ chức quán triệt các quy định về ATTT, nhằm nâng cao nhận thức về trách nhiệm đảm bảo ATTT.

- Cá nhân, tổ chức phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp thiết bị

ii) Với cán bộ quản lý và vận hành hệ thống

- Cán bộ chuyên trách phải thiết lập phương pháp hạn chế truy cập mạng không dây, giám sát và điều khiển truy cập không dây, tổ chức sử dụng chứng thực và mã hóa để bảo vệ truy cập không dây tới hệ thống thông tin.

- Cán bộ chuyên trách phải tổ chức quản lý định danh đối với tất cả người dùng tham gia sử dụng hệ thống thông tin.

b) Định kỳ hàng năng người sử dụng được tổ chức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin theo chương trình, nội dung tại Quyết định số 893/QĐ-TTg ngày 19/6/2015 về việc phê duyệt Đề án Tuyên truyền, phổ biến, nâng cao nhận thức và trách nhiệm về an toàn thông tin đến năm 2020.

c) Định kỳ hàng năng người sử dụng được tổ chức đào tạo các kỹ năng cơ bản về an toàn thông tin theo chương trình, nội dung tại - Quyết định số 99/QĐ-TTg ngày 14/01/2014 phê duyệt Đề án Đào tạo và phát triển nguồn nhân lực an toàn, an ninh thông tin đến năm 2020.

3. Xây dựng các quy định đối với cán bộ nghỉ hoặc thay đổi công việc:

a) Cán bộ nghỉ hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác thuộc sở hữu của tổ chức.

b) Cán bộ quản trị phải vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc.

c) Cán bộ nghỉ hoặc thay đổi công việc phải có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc.

Chương II
BẢO ĐẢM AN TOÀN THÔNG TIN TRONG THUYẾT KẾ, XÂY DỰNG HỆ THỐNG THÔNG TIN

Điều 7. Thiết kế, xây dựng hệ thống thông tin

1. Xây dựng các tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin.

2. Xây dựng các tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin.

3. Xây dựng các tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin.

4. Xây dựng các tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin.

5. Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống.

Điều 8. Phát triển phần mềm thuê khoán

1. Có điều khoản hợp đồng và các cam kết đối với bên thuê khoán khi thực hiện các nội dung liên quan đến việc phát triển phần mềm thuê khoán.

2. Các nhà phát triển cung cấp mã nguồn phần mềm.

3. Phần mềm thuê khoán phải được kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng.

4. Phần mềm thuê khoán phải được kiểm tra, đánh giá an toàn thông tin, trước khi đưa vào sử dụng.

Chương III
BẢO ĐẢM AN TOÀN THÔNG TIN TRONG QUẢN LÝ VẬN HÀNH HỆ THỐNG THÔNG TIN

Điều 9. Quản lý an toàn mạng

1. Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ;

a) Bảo đảm cho hệ điều hành, phần mềm cài đặt trên máy chủ hoạt động liên tục, ổn định và an toàn.

b) Thường xuyên kiểm tra cấu hình, các file nhật ký hoạt động của hệ điều hành, phần mềm nhằm kịp thời phát hiện và xử lý những sự cố nếu có.

c) Quản lý các thay đổi cấu hình kỹ thuật của hệ điều hành, phần mềm.

- Thường xuyên cập nhật các bản vá lỗi hệ điều hành, phần mềm từ nhà cung cấp.

- Loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không còn nhu cầu sử dụng.

- Các bản quyền phần mềm cần được thống kê, quản lý thời gian hạn phục vụ cho việc gia hạn.

2. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố;

Triển khai hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng; phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau; thực hiện sao lưu, dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

3. Truy cập và quản lý cấu hình hệ thống;

a) Cán bộ quản lý, nhân viên vận hành truy cập, khai thác thông tin tại Trung tâm dữ liệu theo trách nhiệm và phân quyền được quy định; việc khai thác thông tin phải bảo đảm nguyên tắc bảo mật, không được tự ý cung cấp thông tin ra bên ngoài.

b) Cán bộ quản lý, nhân viên vận hành có trách nhiệm theo dõi và phát hiện các trường hợp truy cập hệ thống trái phép hoặc thao tác vượt quá giới hạn, báo cáo cho cán bộ quản lý để tiến hành ngăn chặn, thu hồi, khóa quyền truy cập của các tài khoản vi phạm.

c) Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống (cứng hóa) trước khi đưa vào vận hành, khai thác.

d) Quy trình kết nối thiết bị đầu cuối của người sử dụng vào hệ thống mạng; truy nhập và quản lý cấu hình hệ thống; cấu hình tối ưu, tăng cường bảo mật cho

thiết bị mạng, bảo mật (cứng hóa) trong hệ thống và thực hiện quy trình trước khi đưa hệ thống vào vận hành khai thác.

Điều 10. Quản lý an toàn máy chủ và ứng dụng

1. Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ;

a) Bảo đảm cho hệ điều hành, phần mềm cài đặt trên máy chủ hoạt động liên tục, ổn định và an toàn

b) Thường xuyên kiểm tra cấu hình, các file nhật ký hoạt động của hệ điều hành, phần mềm nhằm kịp thời phát hiện và xử lý những sự cố nếu có.

c) Quản lý các thay đổi cấu hình kỹ thuật của hệ điều hành, phần mềm.

- Thường xuyên cập nhật các bản vá lỗi hệ điều hành, phần mềm từ nhà cung cấp.

- Loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không còn nhu cầu sử dụng.

- Các bản quyền phần mềm cần được thống kê, quản lý thời gian hạn phục vụ cho việc gia hạn.

2. Truy cập mạng của máy chủ;

Bảo đảm các kết nối mạng trên máy chủ hoạt động liên tục, ổn định và an toàn. Cấu hình, kiểm soát các kết nối, các cổng dịch vụ từ bên trong đi ra cũng nhưng bên ngoài vào hệ thống.

4. Truy cập và quản trị máy chủ và ứng dụng;

a) Thay đổi các tài khoản, mật khẩu mặc định ngay khi đưa hệ điều hành, phần mềm vào sử dụng

b) Cấp quyền quản lý truy cập của người sử dụng trên máy chủ cài đặt hệ điều hành.

c) Toàn bộ máy chủ và thiết bị công nghệ thông tin không phải máy tính ngoại trừ các hệ thống bắt buộc phải có giao tiếp với Internet (các hệ thống phục vụ truy cập Internet; cung cấp giao diện ra Internet của trang tin điện tử, dịch vụ công, thư điện tử; phục vụ cập nhật bản vá hệ điều hành, mẫu mã độc, mẫu điểm yếu, mẫu tấn công) không được kết nối Internet.

5. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố;

Triển khai hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng; phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau; thực hiện sao lưu, dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

6. Cài đặt, gỡ bỏ hệ điều hành, dịch vụ, phần mềm trên hệ thống máy chủ và ứng dụng;

Đơn vị/bộ phận chuyên trách về công nghệ thông tin của đơn vị chịu trách nhiệm cài đặt phần mềm cho máy tính phục vụ công việc. Người dùng không được can thiệp vào các phần mềm đã cài đặt trên máy tính (thay đổi, gỡ bỏ…) khi chưa được sự đồng ý của bộ phận công nghệ thông tin của đơn vị.

7. Kết nối và gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống;

Cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho hệ thống máy chủ trước khi đưa vào vận hành, khai thác.

8. Các máy chủ trước khi đưa vào vận hành khai thác cần triển khai một số yêu cầu tối ưu và tăng cường bảo mật (cứng hóa) như:

a) Sử dụng hệ điều hành bảo đảm an toàn thông tin.

b) Loại bỏ hoặc tắt tất cả các dịch vụ không cần thiết.

c) Sử dụng các phiên bản phần mềm an toàn.

d) Kiểm soát truy cập và ghi nhận lại hoạt động (log) của tất cả các dịch vụ. Cấm tất cả các truy cập từ bên ngoài vào hệ thống, chỉ cấp quyền truy cập xác đáng cho các người dùng tin cậy.

e) Kiểm soát truy cập ở cấp người dùng cho mỗi dịch vụ.

Điều 11. Quản lý an toàn dữ liệu

1. Yêu cầu an toàn đối với phương pháp mã hóa;

a) Đơn vị phải xây dựng và áp dụng quy định sử dụng các phương thức mã hóa thích hợp theo các chuẩn quốc gia hoặc quốc tế đã được công nhận để bảo vệ thông tin.

b) Phải có biện pháp quản lý khóa mã hóa thích hợp để hỗ trợ việc sử dụng các kỹ thuật mã hóa.

2. Phân loại, quản lý và sử dụng khóa bí mật và dữ liệu mã hóa;

3. Cơ chế mã hóa và kiểm tra tính nguyên vẹn của dữ liệu;

4. Trao đổi dữ liệu qua môi trường mạng và phương tiện lưu trữ;

a) Ban hành quy định về trao đổi thông tin tối thiểu gồm: Phân loại thông tin theo mức độ nhạy cảm; quyền và trách nhiệm của cá nhân khi tiếp cận thông tin; biện pháp đảm bảo tính toàn vẹn, bảo mật khi truyền nhận, xử lý, lưu trữ thông tin; chế độ bảo quản thông tin.

b) Các thông tin, tài liệu, dữ liệu nhạy cảm phải được mã hóa trước khi trao đổi, truyền nhận qua mạng máy tính.

c) Thực hiện các biện pháp quản lý, giám sát và kiểm soát chặt chẽ các trang/cổng thông tin điện tử cung cấp thông tin, dịch vụ, giao dịch trực tuyến cho các tổ chức, cá nhân bên ngoài.

d) Thực hiện biện pháp bảo vệ trang thiết bị, phần mềm phục vụ trao đổi thông tin nội bộ nhằm hạn chế việc xâm nhập, khai thác bất hợp pháp các thông tin nhạy cảm.

5. Sao lưu dự phòng và khôi phục dữ liệu (tần suất sao lưu dự phòng, phương tiện lưu trữ, thời gian lưu trữ; nơi lưu trữ, phương thức lưu trữ và phương thức lấy dữ liệu ra khỏi phương tiện lưu trữ;

a) Lập danh sách các dữ liệu, phần mềm cần được sao lưu, có phân loại theo thời gian lưu trữ, thời gian sao lưu, phương pháp sao lưu và thời gian kiểm tra phục hồi hệ thống từ dữ liệu sao lưu.

b) Xây dựng tài liệu, quy trình hướng dẫn sao lưu/phục hồi dữ liệu của hệ thống: Đơn vị quản trị hệ thống thực hiện xây dựng Tài liệu hướng dẫn sao lưu cụ thể đối với từng hệ thống cung cấp dịch vụ, hệ thống điều hành mà đơn vị quản lý.

6. Cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ;

a) Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ và các thông tin, dữ liệu quan trọng khác trên hệ thống (nếu có).

b) Thực hiện sao lưu dữ liệu định kỳ: Cán bộ phụ trách sao lưu thực hiện sao lưu định kỳ theo phương án sao lưu đã được phê duyệt.

c) Kiểm tra định kỳ: Dữ liệu sao lưu phải được lưu trữ an toàn và được kiểm tra thường xuyên đảm bảo sẵn sàng cho việc sử dụng khi cần. Kiểm tra, phục hồi hệ thống từ dữ liệu sao lưu.

Điều 12. Quản lý an toàn thiết bị đầu cuối

Quy định về quản lý an toàn thiết bị đầu cuối bao gồm các nội dung:

1. Thông tin về thiết bị đầu cuối (tên, chủng loại, địa chỉ MAC, địa chỉ IP) phải được quản lý và cập nhật.

2. Các thiết bị đầu cuối phải được quản lý khi kết nối vào hệ thống mạng theo địa chỉ MAC, IP.

3. Khi truy cập và sử dụng thiết bị đầu cuối từ xa phải có cơ chế xác thực và sử dụng giao thức mạng an toàn.

4. Việc cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống phải được cho phép bởi người có thẩm quyền và thực hiện theo quy trình được phê duyệt.

Điều 13. Quản lý phòng chống phần mềm độc hại

1. Tất cả các máy trạm, máy chủ phải được trang bị phần mềm phòng chống mã độc. Các phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc khi sao chép, mở các tập tin.

2. Khi gửi văn bản điện tử gửi qua hệ thống thư điện tử phải có định dạng theo Danh mục tiêu chuẩn kỹ thuật về ứng dụng CNTT trong cơ quan nhà nước như: (.txt), (.doc), (.odt), (.pdf) và các định dạng khác theo quy định, không được gửi các file thực thi (.com), (.bat), (.exe) ….

3. Các cán bộ, công chức, viên chức và người lao động trong cơ quan phải được hướng dẫn về phòng chống mã độc, các rủi ro do mã độc gây ra; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm trên máy trạm khi chưa có sự đồng ý của người có thẩm quyền theo quy định của cơ quan.

4. Tất cả các máy tính của đơn vị phải được cấu hình nhằm vô hiệu hóa tính năng tự động thực thi (autoplay) các tập tin trên các thiết bị lưu trữ di động.

5. Khi phát hiện ra bất kỳ dấu hiện nào liên quan đến việc bị nhiễm mã độc trên máy trạm (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu…), người sử dụng phải báo trực tiếp cho bộ phận có trách nhiệm của đơn vị để xử lý.

6. Phần mềm ứng dụng trước khi được cài đặt, sử dụng phải được kiểm tra xem có phần mềm độc hại tồn tại hay không? Tất cả các tập tin, thư mục phải được quét mã độc trước khi sao chép, sử dụng.

7. Định kỳ hàng năm thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; Thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống.

Điều 14. Quản lý giám sát an toàn hệ thống thông tin

1. Triển khai hệ thống giám sát trung tâm phải đáp ứng yêu cầu tại khoản 1, Điều 5 Thông tư số 31/2017/TT-BTTTT.

2. Thông tin giám sát và danh mục các đối tượng giám sát phải đáp ứng yêu cầu tại khoản 2, Điều 5 Thông tư số 31/2017/TT-BTTTT. Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát.

3. Thực thi nhiệm vụ giám sát theo quy định tại khoản 3, Điều 5 Thông tư số 31/2017/TT-BTTTT.

4. Định kỳ hàng năm tổ chức nâng cao năng lực hoạt động giám sát theo quy định tại Điều 9 Thông tư số 31/2017/TT-BTTTT.

5. Chủ quản hệ thống thông tin có trách nhiệm giám sát an toàn thông tin theo quy định tại Điều 14 Thông tư số 31/2017/TT-BTTTT.

Điều 15. Quản lý điểm yếu an toàn thông tin

1. Đơn vị/bộ phận chuyên trách về an toàn thông tin có trách nhiệm:

a) Quản lý thông tin điểm yếu an toàn thông tin đối với từng thành phần có trong hệ thống (hệ điều hành, máy chủ, ứng dụng, dịch vụ…); Phân loại mức độ nguy hiểm của điểm yếu; Xây dựng phương án và quy trình xử lý đối với từng mức độ nguy hiểm của điểm yếu.

b) Báo cáo Lãnh đạo/Cán bộ quản lý ngay khi phát hiện điểm yếu an toàn thông tin ở mức độ nghiêm trọng. Thực hiện cảnh báo và xử lý điểm yếu an toàn thông tin theo chỉ đạo. Việc xử lý điểm yếu an toàn thông tin phải bảo đảm không giám ảnh hưởng/gián đoạn hoạt động của hệ thống.

c) Xây dựng phương án xử lý tạm thời đối với trường hợp điểm yếu an toàn thông tin chưa được khắc phục và phương án khôi phục hệ thống trong trường hợp xử lý điểm yếu thất bại.

d) Có trách nhiệm phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu an toàn thông tin đối với các điểm yếu khi cần thiết.

2. Đối với hệ thống/hệ thống thành phần được đề xuất là cấp độ 3 trở lên phải thực hiện kiểm tra, đánh giá và xử lý điểm yếu an toàn thông tin cho thiết bị hệ thống, máy chủ, dịch vụ trước khi đưa vào sử dụng.

3. Định kỳ hàng năm kiểm tra, đánh giá điểm yếu an toàn thông tin cho toàn bộ hệ thống thông tin; Thực hiện quy trình kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin khi có thông tin hoặc nhận được cảnh báo về điểm yếu an toàn thông tin đối với thành phần cụ thể trong hệ thống.

4. Hoạt động đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thực hiện theo quy định tại điểm c khoản 2 Điều 20 Nghị định số 85/2016/NĐ-CP và Điều 13 Thông tư số 03/2017/TT-BTTTT

Điều 16. Quản lý sự cố an toàn thông tin

1. Phân nhóm sự cố an toàn thông tin, bao gồm:

a) Sự cố do bị tấn công mạng: tấn công từ chối dịch vụ; tấn công giả mạo; tấn công sử dụng mã độc; truy cập trái phép, chiếm quyền điều khiển; tấn công thay đổi giao diện; tấn công mã hóa phần mềm, dữ liệu, thiết bị; phá hoại thông tin, dữ liệu, phần mềm; nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu; các hình thức tấn công mạng khác.

b) Hỏng hóc phần cứng, lỗi phần mềm của hệ thống thông tin làm mất tính sẵn sàng của hệ thống thông tin.

c) Hỏng hóc, lỗi của các hệ thống thuộc hạ tầng Trung tâm dữ liệu, phòng máy chủ (nguồn điện, làm mát, chống sét, chống cháy...) làm mất tính sẵn sàng của hệ thống thông tin.

d) Hỏng hóc, lỗi của hệ thống mạng làm mất khả năng truy cập tới hệ thống thông tin của các đối tượng sử dụng hệ thống.

đ) Sự cố do lỗi của người quản trị, vận hành hệ thống.

e) Sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn.

Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin: Hoạt động ứng cứu sự cố an toàn thông tin mạng huy động các nguồn lực nằm ngoài phạm vi của đơn vị vận hành hệ thống thông tin để đối phó với các sự cố quy định tại khoản 1 điều này.

2. Kế hoạch ứng phó sự cố an toàn thông tin;

a) Chủ quản HTTT chỉ đạo Đơn vị vận hành tổ chức xây dựng, phê duyệt Kế hoạch ứng phó sự cố cho các hệ thống thông tin do đơn vị trực tiếp quản lý theo đề cương tại Phụ lục II Quyết định số 05/2017/QĐ-TTg (bao gồm các điều chỉnh do Bộ Thông tin và Truyền thông ban hành nếu có) và tổ chức triển khai kế hoạch sau khi phê duyệt. Đối với các nội dung trong kế hoạch vượt thẩm quyền quyết định của đơn vị, đơn vị lấy ý kiến của đơn vị chuyên trách ATTT (đối với các nội dung yêu cầu có kinh phí), báo cáo chủ quản HTTT xem xét, quyết định.

b) Các kế hoạch ứng phó sự cố sau khi được phê duyệt phải gửi đơn vị chuyên trách ATTT tổng hợp thành kế hoạch chung toàn hệ thống, trình chủ quản HTTT phê duyệt.

c) Kế hoạch ứng phó sự cố được rà soát và điều chỉnh hàng năm (nếu cần thiết) trước ngày 31 tháng 10, làm cơ sở để xây dựng kế hoạch bảo đảm an toàn thông tin năm tiếp theo.

3. Đơn vị/bộ phận chuyên trách về an toàn thông tin có trách nhiệm

a) Phân nhóm sự cố an toàn thông tin mạng theo quy định tại Quyết định số 05/2017/NĐ-CP của Thủ tướng Chính phủ ngày 16/3/2017 quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia (Quyết định 05); Xây dựng phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng, ứng phó sự cố an toàn thông tin mạng.

b) Xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13,14 Quyết định số 05.

c) Xây dựng và triển khai kế hoạch ứng phó sự cố an toàn thông tin theo quy định tại Điều 16 Quyết định số 05.

d) Quyết định toàn diện về mặt kỹ thuật đối với các cơ quan trong quá trình khắc phục sự cố về ATTT; Hỗ trợ, phối hợp và hướng dẫn các cơ quan khắc phục sự cố mất ATTT; Yêu cầu ngưng hoạt động một phần hoặc toàn bộ các hệ thống thông tin của các cơ quan nhằm phục vụ công tác khắc phục sự cố về ATTT; Phối hợp với đơn vị chức năng trong điều tra các nguyên nhân gây ra sự cố mất an toàn thông tin theo chỉ đạo của Lãnh đạo.

đ) Phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin; Yêu cầu bên cung cấp, hỗ trợ cung cấp quy trình xử lý sự cố cho các dịch vụ do bên cung cấp, hỗ trợ cung cấp liên quan đến hệ thống.

e) Tổ chức diễn tập phương án xử lý sự cố an toàn thông tin theo chỉ đạo của Lãnh đạo.

4. Trách nhiệm của người dùng

Thông tin, báo cáo kịp thời cho cán bộ chuyên trách về ATTT của cơ quan khi phát hiện các sự cố gây mất ATTT trong quá trình tham gia vào hệ thống thông tin của đơn vị; Phối hợp tích cực trong suốt quá trình giải quyết và khắc phục sự cố.

Điều 17. Quản lý an toàn người sử dụng đầu cuối

1. Kết nối máy tính/thiết bị đầu cuối của người sử dụng vào hệ thống:

a) Người sử dụng khi truy cập, sử dụng tài nguyên nội bộ, truy cập mạng và tài nguyên trên Internet phải tuân thủ các quy định của pháp luật về bảo đảm an toàn thông tin và các quy định của cơ quan, tổ chức.

b) Khi cài đặt, kết nối máy tính/thiết bị đầu cuối phải thực hiện theo hướng dẫn/quy trình dưới sự giám sát của bộ phận chuyên trách về an toàn thông tin.

c) Đối với hệ thống thông tin có cấp độ 3 trở lên, máy tính/thiết bị đầu cuối phải được xử lý điểm yếu an toàn thông tin, cấu hình cứng hóa bảo mật trước khi kết nối vào hệ thống.

2. Trong quá trình sử dụng:

a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao;

b) Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng;

c) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách công nghệ thông tin của cơ quan, đơn vị để kịp thời ngăn chặn và xử lý;

d) Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng được tỉnh hoặc đơn vị chuyên môn tổ chức.

Chương IV
KIỂM TRA, ĐÁNH GIÁ VÀ QUẢN LÝ RỦI RO

Điều 18. Nội dung, hình thức kiểm tra, đánh giá

1. Nội dung kiểm tra, đánh giá:

a) Kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ;

b) Đánh giá hiệu quả của biện pháp bảo đảm an toàn hệ thống thông tin;

c) Đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống;

d) Kiểm tra, đánh giá khác do chủ quản hệ thống thông tin quy định.

2. Hình thức kiểm tra, đánh giá:

a) Kiểm tra, đánh giá định kỳ theo kế hoạch của chủ quản hệ thống thông tin;

b) Kiểm tra, đánh giá đột xuất theo yêu cầu của cấp có thẩm quyền.

3. Cấp có thẩm quyền yêu cầu kiểm tra, đánh giá:

a) Đơn vị chuyên trách ATTT tại Trung ương;

b) UBND tỉnh;

c) Sở Thông tin và Truyền thông đối với hệ thống thông tin do đơn vị này phê duyệt hồ sơ đề xuất cấp độ.

4. Đơn vị chủ trì kiểm tra, đánh giá là đơn vị được cấp có thẩm quyền giao nhiệm vụ hoặc được lựa chọn để thực hiện nhiệm vụ kiểm tra, đánh giá.

5. Đối tượng kiểm tra, đánh giá là chủ quản hệ thống thông tin hoặc đơn vị vận hành hệ thống thông tin và các hệ thống thông tin có liên quan.

Điều 19. Kiểm tra việc tuân thủ quy định về an toàn thông tin và hiệu quả của biện pháp bảo đảm an toàn thông tin

1. Nội dung kiểm tra, đánh giá

a) Kiểm tra việc xác định cấp độ an toàn hệ thống thông tin và triển khai phương án bảo đảm an toàn thông tin; Kiểm tra hiệu quả của các biện pháp bảo đảm an toàn thông tin.

b) Kiểm tra công tác giám sát an toàn thông tin; ứng cứu sự cố an toàn thông tin.

c) Kiểm tra các nội dung khác tại quy chế.

2. Thẩm quyền kiểm tra

a) Sở Thông tin và Truyền thông chịu trách nhiệm kiểm tra các cơ quan, đơn vị thuộc UBND Tỉnh.

b) Các đơn vị khác tự kiểm tra trong nội bộ đơn vị.

3. Hoạt động kiểm tra về an toàn thông tin do Sở Thông tin và Truyền thông thực hiện tại các đơn vị thuộc công tác ứng dụng công nghệ thông tin hàng năm, theo kế hoạch được UBND tỉnh phê duyệt. Hoạt động kiểm tra về an toàn thông tin do các cơ quan, đơn vị trong địa bàn tỉnh thực hiện có thể lồng ghép trong chương trình kiểm tra công tác ứng dụng công nghệ thông tin hàng năm, theo kế hoạch được Lãnh đạo đơn vị phê duyệt.

Chương V
BÁO CÁO, CHIA SẺ THÔNG TIN

Điều 20. Chế độ báo cáo

1. Báo cáo định kỳ:

a) Báo cáo an toàn thông tin định kỳ hàng năm gồm các nội dung quy định tại khoản 3 Điều 17 Thông tư 03/2017/TT-BTTTT.

b) Báo cáo hoạt động giám sát của chủ quản hệ thống thông tin định kỳ 6 tháng theo mẫu tại Phụ lục 2 Thông tư 31/2017/TT-BTTTT.

2. Báo cáo đột xuất: Báo cáo về công tác khắc phục mã độc, lỗ hổng, điểm yếu, triển khai cảnh báo an toàn thông tin và các báo cáo đột xuất khác theo yêu cầu của các cơ quan quản lý nhà nước về an toàn thông tin.

3. Trách nhiệm lập, phê duyệt báo cáo

a) Các cơ quan, đơn vị sự nghiệp trong địa bàn tỉnh chịu trách nhiệm:

- Lập báo cáo an toàn thông tin theo quy định tại điểm a khoản 1 điều này, gửi Sở Thông tin và Truyền thông trước ngày 15 tháng 11 hàng năm.

- Lập báo cáo hoạt động giám sát của chủ quản hệ thống thông tin theo quy định tại điểm b khoản 1 điều này, gửi Sở Thông tin và Truyền thông trước ngày 15 tháng 6 và 15 tháng 12 hàng năm.

- Báo cáo đột xuất theo hướng dẫn của Sở Thông tin và Truyền thông.

b) Sở Thông tin và Truyền thông chịu trách nhiệm tập hợp, tổng hợp báo cáo của các đơn vị, trình Bộ phê duyệt, gửi các cơ quan quản lý nhà nước về an toàn thông tin.

Điều 21. Chia sẻ thông tin

1. Việc chia sẻ thông tin về công tác bảo đảm an toàn thông tin với các đơn vị ngoài Bộ được thực hiện theo quy định tại Điều 18 Thông tư 03/2017/TT-BTTT.

2. Khuyến khích các đơn vị trong địa bàn tỉnh chia sẻ kinh nghiệm triển khai, vận hành hệ thống an toàn thông tin thông qua trao đổi trực tiếp giữa các đơn vị hoặc hội thảo nội bộ.

3. Sở Thông tin và Truyền thông chịu trách nhiệm tổ chức hội thảo trao đổi kinh nghiệm giữa các đơn vị trong địa bàn tỉnh tối thiểu 2 năm 1 lần.

Chương VI
TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 22. Đơn vị vận hành

a) Thực hiện trách nhiệm của đơn vị vận hành hệ thống thông tin theo quy định tại quy chế này và các nhiệm vụ do chủ quản hệ thống thông tin phân công.

b) Chỉ đạo, phân công các bộ phận kỹ thuật thuộc đơn vị (quản lý ứng dụng; quản lý dữ liệu; vận hành hệ thống thông tin; triển khai và hỗ trợ kỹ thuật) triển khai công tác bảo đảm an toàn thông tin trong tất cả các công đoạn liên quan đến hệ thống thông tin.

Điều 23. Trách nhiệm của Sở TT&TT

a) Thực hiện các trách nhiệm được giao tại quy chế này.

b) Hướng dẫn triển khai quy chế này và các quy định liên quan của Nhà nước.

c) Tổ chức triển khai thực hiện quy chế tại các cơ quan, đơn vị thuộc UBND tỉnh.

d) Xây dựng kế hoạch, báo cáo về an toàn thông tin mạng trong địa bàn tỉnh.

Điều 24. Các đơn vị khác trên địa bàn

a) Thực hiện trách nhiệm của chủ quản hệ thống thông tin hoặc đơn vị quản lý trực tiếp hệ thống thông tin trong trường hợp có hệ thống thông tin thuộc quản lý trực tiếp của đơn vị theo quy định của quy chế này.

b) Tổ chức triển khai thực hiện quy chế này tại đơn vị.

c) Thực hiện các báo cáo về an toàn thông tin mạng khi được Sở Thông tin và Truyền thông yêu cầu.

Chương VII
TỔ CHỨC THỰC HIỆN

Điều 25. Tổ chức triển khai quy chế

Quy định này có hiệu lực thi hành kể từ ngày ký ban hành.

Trong quá trình thực hiện nếu có vấn đề phát sinh, vướng mắc, các đơn vị liên quan phản ánh kịp thời về Đơn vị chuyên trách để xem xét, bổ sung, sửa đổi.

Điều 26. Rà soát, cập nhật, bổ sung quy chế

1. Định kỳ 02 năm hoặc khi có thay đổi quy chế bảo đảm an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung.

2. Trong quá trình thực hiện quy chế, nếu có vấn đề vướng mắc, phát sinh, các đơn vị phản ánh kịp thời về Sở Thông tin và Truyền thông để tổng hợp báo cáo Uỷ ban nhân dân tỉnh điều chỉnh, bổ sung./.