UBND TỈNH GIA LAI
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số:1017/STTTT-CNTT
V/v hướng dẫn bảo đảm an toàn hệ thống thông tin theo cấp độ

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

Gia Lai, ngày 09 tháng 8 năm 2019

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

Thực hiện Chỉ thị số 14/CT-TTg ngày 07/6/2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam và hướng dẫn của Cục An toàn thông tin – Bộ Thông tin và Truyền thông tại Công văn số 713/CATTT-TĐQLGS ngày 25/7/2019 về việc hướng dẫn xác định và thực thi bảo vệ hệ thống thông tin theo cấp độ, nhằm thực hiện nhiệm vụ được giao và tăng cường công tác đảm bảo an toàn thông tin mạng của các cơ quan, đơn vị trên địa bàn tỉnh, Sở Thông tin và Truyền thông hướng dẫn các cơ quan, đơn vị triển khai thực hiện các nội dung sau:

1. Xác định cấp độ an toàn hệ thống thông tin và trách nhiệm bảo đảm an toàn hệ thống thông tin theo từng cấp độ đối với các hệ thống thông tin thuộc phạm vi quản lý, vận hành của đơn vị, địa phương (theo quy định tại Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ; Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông).

2. Đơn vị vận hành hệ thống thông tin xây dựng Hồ sơ đề xuất cấp độ (hồ sơ theo Phụ lục II của Công văn này):

2.1. Đối với hệ thống thông tin được đề xuất là cấp độ 1 hoặc cấp độ 2: gửi hồ sơ đến Đơn vị chuyên trách về an toàn thông tin của Chủ quản hệ thống thông tin thực hiện thẩm định, phê duyệt.

2.2. Đối với hệ thống thông tin được đề xuất là cấp độ 3: gửi hồ sơ đến Đơn vị chuyên trách về an toàn thông tin của Chủ quản hệ thống thông tin thực hiện thẩm định, sau đó trình Chủ quản hệ thống thông tin để phê duyệt.

2.3. Đối với hệ thống thông tin được đề xuất là cấp độ 4:

- Gửi hồ sơ đến Đơn vị chuyên trách về an toàn thông tin của Chủ quản hệ thống thông tin hoặc Sở Thông tin và Truyền thông để tham gia ý kiến chuyên môn.

- Sau khi có ý kiến chuyên môn của Đơn vị chuyên trách về an toàn thông tin của Chủ quản hệ thống thông tin hoặc Sở Thông tin và Truyền thông, Đơn vị vận hành hệ thống thông tin trình Chủ quản hệ thống thông tin hồ sơ đề xuất cấp độ để gửi tới Bộ Thông tin và Truyền thông chủ trì, phối hợp với Bộ Quốc phòng, Bộ Công an và các bộ, ngành liên quan thực hiện thẩm định hồ sơ đề xuất cấp độ.

2.5. Đối với hệ thống thông tin có nhiều hệ thống thành phần hoặc phân tán, có nhiều hơn một đơn vị vận hành hệ thống thông tin thì đơn vị làm đầu mối thực hiện

quyền và nghĩa vụ vủa đơn vị vận hành hệ thống thông tin, theo đó đối với các hệ thống thông tin dùng chung đang vận hành tại Trung tâm Tích hợp dữ liệu tỉnh Gia Lai như: hệ thống Quản lý văn bản và điều hành (3 cấp) dùng chung của tỉnh, hệ thống Một cửa điện tử liên thông (dùng chung), hệ thống mạng diện rộng WAN, hệ thống Hội nghị truyền hình trực tuyến...do Sở Thông tin và Truyền thông trình UBND tỉnh phê duyệt cấp độ an toàn hệ thống thông tin. Các cơ quan, đơn vị, địa phương là một trong số các đơn vị thành phần tham gia vận hành các hệ thống nêu trên, khi thực hiện xác định và phê duyệt cấp độ an toàn hệ thống thông tin cho các hệ thống thông tin tại đơn vị mình thì không cần thực hiện xác định cấp độ đối với các hệ thống này.

Trong đó, phương án bảo đảm an toàn thông tin trong Hồ sơ đề xuất phải đáp ứng các yêu cầu an toàn theo tiêu chuẩn quốc gia TCVN 11930:2017 về yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ, trình cấp có thẩm quyền phê duyệt theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

3. Tổ chức triển khai phương án bảo đảm an toàn thông tin theo phương án thuyết minh trong Hồ sơ đề xuất cấp độ sau khi được phê duyệt.

4. Thời hạn thực hiện và báo cáo kết quả về Sở Thông tin và Truyền thông: **trước ngày 30/11/2019** để tổng hợp báo cáo UBND tỉnh.

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

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

- Phụ lục II: Hướng dẫn lập, thẩm định hồ sơ đề xuất cấp độ an toàn hệ thống thông tin; bảo vệ hệ thống thông tin theo cấp độ và hồ sơ tham khảo.

- Phụ lục III: Các biểu mẫu văn bản.

- Hướng dẫn của Cục An toàn thông tin – Bộ Thông tin và Truyền thông tại Công văn số 713/CATTT-TĐQLGS ngày 25/7/2019 về việc hướng dẫn xác định và thực thi bảo vệ hệ thống thông tin theo cấp độ.

Tài liệu được đăng tải trên Trang thông tin điện tử tại địa chỉ: http://stttt.gialai.gov.vn, chuyên mục An toàn thông tin mạng.

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

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

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

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Đặng Quang Khanh

PHỤ LỤC I:
MỘT SỐ NỘI DUNG HƯỚNG DẪN TRIỂN KHAI THỰC HIỆN

(Kèm theo Công văn số 1017/STTTT-CNTT ngày 09/8/2019 của Sở Thông tin và Truyền thông)

1. Các thuật ngữ về *Chủ quản hệ thống thông tin, Đơn vị vận hành hệ thống thông tin, Đơn vị chuyên trách về công nghệ thông tin, Đơn vị chuyên trách về an toàn thông tin, Bộ phận chuyên trách về an toàn thông tin* được định nghĩa, giải thích tại Điều 3 Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn thông tin theo cấp độ (gọi tắt là Nghị định số 85/2016/NĐ-CP) và Điều 5, Điều 6 Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ (gọi tắt là Thông tư số 03/2017/TT-BTTTT) và theo hướng dẫn của Cục An toàn thông tin – Bộ Thông tin và Truyền thông tại Công văn số 713/CATTT-TĐQLGS.

2. Việc phân loại thông tin và hệ thống thông tin được quy định tại Điều 6 Nghị định số 85/2016/NĐ-CP và hướng dẫn tại Điều 4 Thông tư số 03/2017/TT-BTTTT; nguyên tắc xác định cấp độ, việc xác định cấp độ và thuyết minh cấp độ an toàn hệ thống thông tin thực hiện theo quy định tại Điều 5, Điều 7, Điều 8, Điều 9, Điều 10, Điều 11 Nghị định số 85/2016/NĐ-CP và hướng dẫn tại Điều 7 Thông tư số 03/2017/TT-BTTTT; việc xây dựng phương án bảo đảm an toàn thông tin theo cấp độ tương ứng phải đáp ứng các yêu cầu, nội dung quy định tại Điều 19 Nghị định số 85/2016/NĐ-CP và hướng dẫn tại Điều 8, Điều 9 Thông tư số 03/2017/TT-BTTTT và hướng dẫn của Cục An toàn thông tin – Bộ Thông tin và Truyền thông tại Công văn số 713/CATTT-TĐQLGS.

3. 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 đơn vị, địa phương 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 thực hiện theo quy định tại Điều 20 Nghị định 85/2016/NĐ-CP: Chỉ định đơn vị chuyên trách về công nghệ thông tin làm nhiệm vụ đơn vị chuyên trách về an toàn thông tin (đối với cấp huyện, theo quy định tại Thông tư liên tịch 06/2016/TTLT-BTTTT-BNV, Phòng Văn hóa và Thông tin là đơn vị chuyên trách về công nghệ thông tin tại địa phương) hoặc thành lập, chỉ định bộ phận chuyên trách về an toàn thông tin trực thuộc đơn vị chuyên trách về công nghệ thông tin (đối với đơn vị, sở, ban, ngành, theo quy định tại Điểm b, Khoản 2, Điều 25, Luật An toàn thông tin mạng: Chủ quản hệ thống thông tin thực hiện: Chỉ định cá nhân, bộ phận phụ trách về an toàn thông tin mạng; do đó các đơn vị có thể thành lập, chỉ định bộ phận chuyên trách về an toàn thông tin mạng là bộ phận/phòng/ban/đơn vị phụ trách về công nghệ thông tin của đơn vị mình).

4. Thẩm quyền thẩm định và phê duyệt cấp độ; hồ sơ đề xuất cấp độ, hồ sơ phê duyệt đề xuất cấp độ; trình tự thủ tục xác định, xác định lại cấp độ, thẩm định, phê

duyệt hồ sơ đề xuất cấp độ an toàn hệ thống thông tin được quy định từ Điều 12 đến Điều 18 Nghị định số 85/2016/NĐ-CP và hướng dẫn từ Điều 14 đến Điều 16 Thông tư số 03/2017/TT-BTTTT:

- Đối với hệ thống thông tin có chủ quản là UBND cấp huyện *(có thẩm quyền quyết định đầu tư dự án xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin)* thì đơn vị chuyên trách về an toàn thông tin hoặc bộ phận chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin thực hiện thẩm định, phê duyệt hồ sơ đề xuất cấp độ đối với hệ thống thông tin được đề xuất là cấp độ 1 hoặc cấp độ 2. Đối với cấp độ 3 thì đơn vị chuyên trách về an toàn thông tin hoặc bộ phận chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin thực hiện thẩm định hồ sơ đề xuất cấp độ, trình UBND cấp huyện - chủ quản hệ thống thông tin phê duyệt hồ sơ đề xuất cấp độ.

- Đối với hệ thống thông tin có chủ quản là các sở, ban, ngành *(có thẩm quyền quyết định đầu tư dự án xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin)* thì đơn vị chuyên trách về an toàn thông tin hoặc bộ phận chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin thực hiện thẩm định, phê duyệt hồ sơ đề xuất cấp độ đối với hệ thống thông tin được đề xuất là cấp độ 1 hoặc cấp độ 2. Đối với cấp độ 3 thì đơn vị chuyên trách về an toàn thông tin hoặc bộ phận chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin thực hiện thẩm định hồ sơ đề xuất cấp độ, trình Lãnh đạo các sở, ban, ngành - chủ quản hệ thống thông tin phê duyệt hồ sơ đề xuất cấp độ.

- Đối với hệ thống thông tin có chủ quản là UBND tỉnh *(cấp có thẩm quyền quyết định đầu tư dự án xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin)* thì Sở Thông tin và Truyền thông là đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin thực hiện thẩm định, phê duyệt hồ sơ đề xuất cấp độ đối với hệ thống thông tin được đề xuất là cấp độ 1 hoặc cấp độ 2. Đối với cấp độ 3 thì Sở Thông tin và Truyền thông thực hiện thẩm định hồ sơ đề xuất cấp độ, trình UBND tỉnh - chủ quản hệ thống thông tin phê duyệt hồ sơ đề xuất cấp độ.

4. Đối với hệ thống thông tin được đề xuất cấp độ 1, 2, 3 của các cơ quan, đơn vị, đề nghị Đơn vị vận hành hệ thông thông tin lập hồ sơ theo mẫu hướng dẫn tại Phụ lục II *(gửi kèm theo, mục 1.1.3)* gửi về đơn vị có thẩm quyền thẩm định, phê duyệt 01 bản chính và 02 bản sao hồ sơ hợp lệ để thẩm định theo quy định, hướng dẫn tại khoản 3, 4 nêu trên.

5. Đối với hệ thống thông tin được đề xuất cấp độ 4 của các cơ quan, đơn vị, Đơn vị vận hành hệ thống thông tin lập hồ sơ theo mẫu hướng dẫn tại Phụ lục II *(gửi kèm theo, mục 1.1.3)* để gửi đơn vị chuyên trách về an toàn thông tin xem xét, có ý kiến. Sau đó trình chủ quản hệ thống thông tin để trình Bộ Thông tin và Truyền thông thẩm định trước khi chủ quản hệ thống thông tin phê duyệt cấp độ.

(Quy định chi tiết tại Chương IV của Công văn số 713/CATTT-TĐQLGS ngày 25/7/2019 của Cục An toàn thông tin – Bộ Thông tin và Truyền thông)

PHỤ LỤC II: HƯỚNG DẪN LẬP, THẨM ĐỊNH HỒ SƠ ĐỀ XUẤT CẤP ĐỘ AN TOÀN HỆ THỐNG THÔNG TIN; BẢO VỆ HỆ THỐNG THÔNG TIN THEO CẤP ĐỘ VÀ HỒ SƠ THAM KHẢO

(K*èm theo Công văn số 1017/STTTT-CNTT ngày 09/8/2019 của Sở Thông tin và Truyền thông*)

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

(Theo hướng dẫn tại Chương V của Công văn số 713/CATTT-TĐQLGS ngày 25/7/2019 của Cục An toàn thông tin – Bộ Thông tin và Truyền thông)

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

(Theo hướng dẫn tại Chương VI của Công văn số 713/CATTT-TĐQLGS ngày 25/7/2019 của Cục An toàn thông tin – Bộ Thông tin và Truyền thông)

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

3.1. 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.

3.2. 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.

3.3. 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.

3.4. 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.

3.5. 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.

3.6. 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.

❖ **Hồ sơ đề xuất cấp độ, tham khảo theo mẫu sau:**

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

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

Gia Lai – tháng ….năm 2019

PHẦN I
THUYẾT MINH TỔNG QUAN VỀ HỆ THỐNG THÔNG TIN

1. Thông tin Chủ quản hệ thống thông tin

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

- Tên Tổ chức: (Ví dụ) Cơ quan A.
- Số Quyết định thành lập/Quy định chức năng, nhiệm vụ và quyền hạn.
- Người đại diện: Họ và tên, chức vụ.
- Địa chỉ: Địa chỉ trụ sở cơ quan.
- Thông tin liên hệ: Số điện thoại, thư điện tử.

2. Thông tin Đơn vị vận hành

***Hướng dẫn**: Cung cấp thông tin về đơn vị vận hành, bao gồm:*

- Tên Đơn vị vận hành: (Ví dụ) Đơn vị A.
- Số Quyết định thành lập/Quy định chức năng, nhiệm vụ và quyền hạn.
- Người đại diện: Họ và tên, chức vụ.
- Địa chỉ: Địa chỉ trụ sở của đơn vị.
- Thông tin liên hệ: Số điện thoại, thư điện tử.

3. Mô tả phạm vi, quy mô của hệ thống

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

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

- Đối tượng phục vụ của hệ thống: Cơ quan, tổ chức, doanh nghiệp, người dân của địa phương/cơ quan A.

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

+ Phòng máy chủ/Trung tâm tích hợp dữ liệu của cơ quan, đơn vị.

+ Hệ thống Cổng/Trang thông tin điện tử.

+ Hệ thống Quản lý văn bản và điều hành.

+ Hệ thống Một cửa điện tử.

+ Hệ thống Quản lý lưu trữ.

+ Hệ thống quản lý công tác thanh tra.

+ Hệ thống mạng nội bộ - LAN của cơ quan.

…

4. Mô tả cấu trúc của hệ thống

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

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

Trường hợp các hệ thống thông tin có cấu trúc đặc thù theo chức năng và không có những vùng mạng được đưa ra như trong Thông tư số 03/2017/TT-BTTTT của Bộ TT&TT về quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ (gọi tắt là Thông tư 03) thì việc mô tả cấu trúc của hệ thống thông tin đó được mô tả theo cấu trúc thực tế của hệ thống.

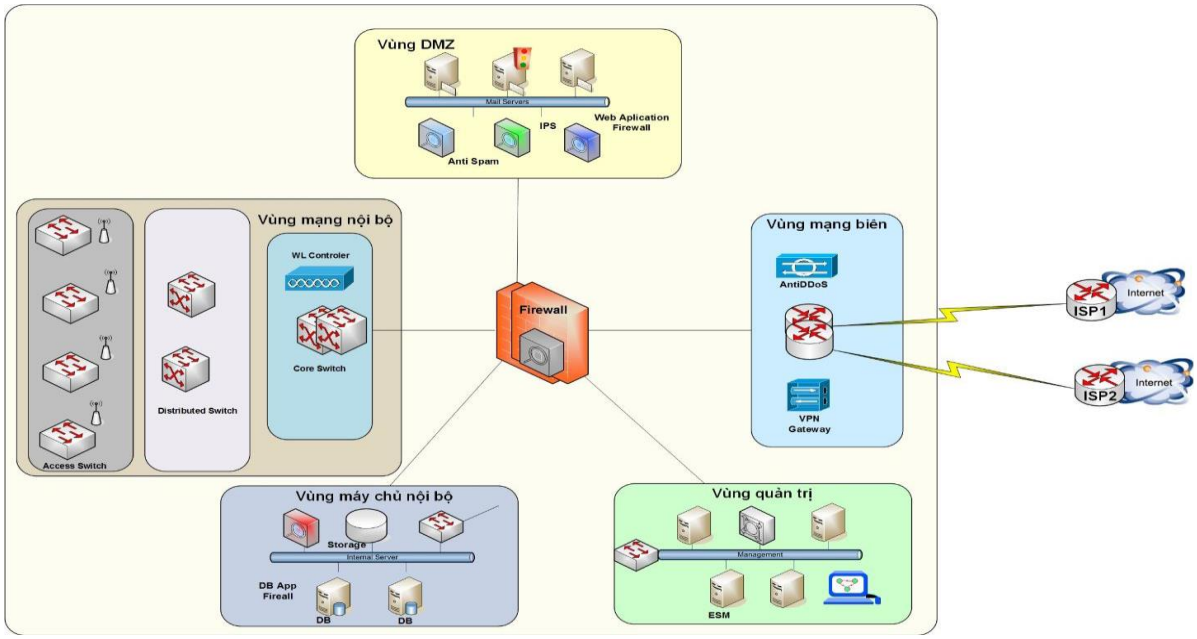
b) Cấu trúc vật lý mô tả các thiết bị mạng, các thiết bị đầu cuối có trong hệ thống và các kết nối vật lý giữa các thiết bị.

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

d) Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống (bao gồm các ứng dụng nghiệp vụ như quản lý văn bản và điều hành, một cửa điện tử,… và các dịch vụ hệ thống như DNS, DHCP, FTP…): Cung cấp thông tin các ứng dụng/dịch vụ có trên hệ thống bao gồm Tên dịch vụ; Máy chủ triển khai/Vị trí triển khai/Hệ điều hành máy chủ; Mục đích sử dụng dịch vụ.

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

4.1. Sơ đồ logic tổng thể



Hình 1: Cấu trúc logic của hệ thống A

Các vùng mạng được thiết kế như sau:

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

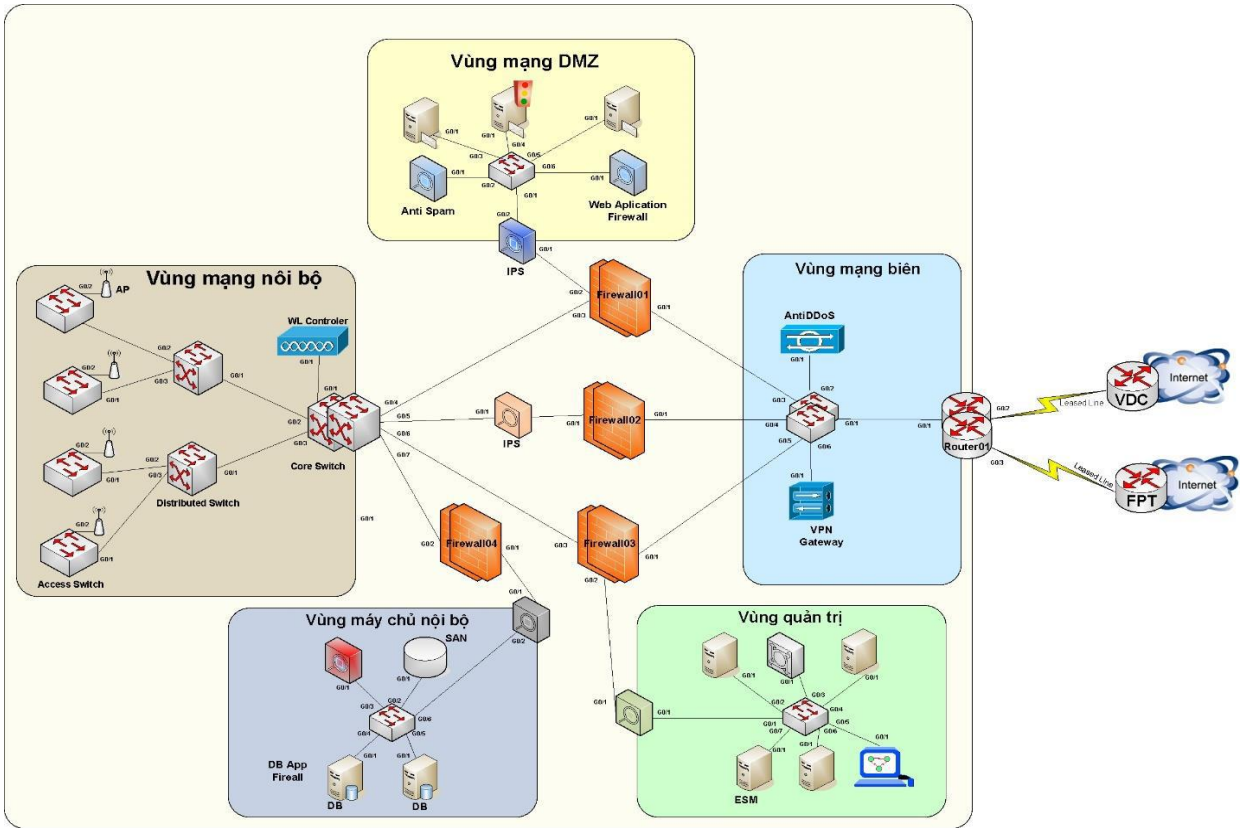
+ Vùng DMZ đặt các máy chủ công cộng, cung cấp dịch vụ ra bên ngoài Internet. Vùng mạng này triển khai thiết bị phòng chống xâm nhập IPS, thiết bị Web Application Firewall, thiết bị Anti-Spam.

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

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

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

4.2. Sơ đồ kết nối vật lý



Hình 2: Kết nối vật lý của Hệ thống A

4.3. Danh mục thiết bị sử dụng trong hệ thống

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

	OS		vùng mạng DMZ
3	…	…	….

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

STT	Tên dịch vụ	Máy chủ triển khai	Mục đích sử dụng
1	Hệ thống quản lý văn bản và điều hành	Máy chủ Noibo01/ Vùng máy chủ nội bộ/ WindowServer 2012	Cung cấp ứng dụng quản lý văn bản cho cán bộ bên trong hệ thống; kết nối, liên thông với các hệ thống liên quan
2	Hệ thống thông tin một cửa điện tử	Máy chủ Noibo02/ Vùng máy chủ nội bộ/ Centos7	Cung cấp ứng dụng theo dõi, quản lý thông tin tiếp nhận, giải quyết TTHC bên trong hệ thống và cung cấp thông tin công khai về DVCTT, tình trạng giải quyết TTHC cho người sử dụng bên ngoài Internet
3	Hệ thống mạng nội bộ	Máy chủ Noibo03/ Vùng máy chủ nội bộ/ Centos7	Cung cấp truy cập nội bộ các ứng dụng, thư mục lưu trữ.
4	…	…	…

4.5. 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 ĐỀ XUẤT CẤP ĐỘ AN TOÀN HỆ THỐNG THÔNG TIN

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

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

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

Trường hợp một hệ thống thông tin lớn, bao gồm nhiều thành phần khác nhau, thì cần xác định loại thông tin và loại hình của từng thành phần tương ứng. Thành

phần nào có tiêu chí để đề xuất cấp độ cao nhất sẽ quyết định cấp độ an toàn thông tin của hệ thống đó. Do đó, khi xác định cấp độ của Hệ thống thông tin cần xác định thành phần nào trong hệ thống thông tin tổng thể khớp với tiêu chí xác định cấp độ ở cấp cao nhất.

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

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

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

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

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

STT	Hệ thống	Loại thông tin xử lý	Loại hình HTTT	Cấp độ đề xuất	Căn cứ đề xuất
1	Phòng máy chủ/Trung tâm tích hợp dữ liệu của cơ quan, đơn vị		Hệ thống cơ sở hạ tầng thông tin dùng chung phục vụ hoạt động của một cơ quan, tổ chức.	2	Khoản 3, Điều 8 Nghị định số 85/2016/NĐ-CP
2	Phòng máy chủ/Trung tâm tích hợp dữ liệu của cơ quan, đơn vị		Hệ thống cơ sở hạ tầng thông tin dùng chung phục vụ hoạt động của một cơ quan, tổ chức.	3	Khoản 3, Điều 9 Nghị định số 85/2016/NĐ-CP
3	Hệ thống quản lý văn bản và điều hành của tỉnh	Thông tin riêng	Hệ thống thông tin phục vụ hoạt động nội bộ các	2	Khoản 1, Điều 8 Nghị định số 85/2016/NĐ-CP

			cơ quan nhà nước của tỉnh		
4	Hệ thống một cửa điện tử của tỉnh	Thông tin riêng	Hệ thống thông tin phục vụ hoạt động nội bộ các cơ quan nhà nước của tỉnh	2	Khoản 1, Điều 8 Nghị định số 85/2016/NĐ-CP
5	Cổng/Trang thông tin điện tử của cơ quan, đơn vị	Thông tin công cộng	Hệ thống thông tin phục vụ người dân, doanh nghiệp, cung cấp thông tin và DVC trực tuyến từ mức độ 2 trở xuống	2	Điểm a, Khoản 2, Điều 8 Nghị định số 85/2016/NĐ-CP
6	Hệ thống quản lý CBCCVC	Thông tin riêng	Hệ thống thông tin phục vụ hoạt động nội bộ các cơ quan nhà nước của tỉnh	2	Khoản 1, Điều 8 Nghị định số 85/2016/NĐ-CP
7	Hệ thống mạng nội bộ - LAN của cơ quan		Hệ thống cơ sở hạ tầng thông tin phục vụ hoạt động của cơ quan	2	Khoản 3, Điều 8 Nghị định số 85/2016/NĐ-CP
8	Hệ thống Dịch vụ công trực tuyến	Thông tin công cộng	Hệ thống thông tin phục vụ người dân, doanh nghiệp	3	Điểm a, Khoản 2, Điều 9 Nghị định số 85/2016/NĐ-CP
…					

2. Thuyết minh 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 địa phương/cơ quan A. Căn cứ theo quy định tại Khoản 1/Điều 7/NĐ85, hệ thống này được đề xuất cấp độ 1.

Hoặc 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 địa phương/cơ quan A. Căn cứ theo quy định tại Khoản 3, Điều 8 Nghị định số 85/2016/NĐ-CP, hệ thống này được đề xuất cấp độ 2.

2.2. Hệ thống Quản lý văn bản và điều hành

Hệ thống quản lý văn bản có xử lý thông tin riêng của địa phương/cơ quan A và phục vụ hoạt động nội bộ cho cán bộ của địa phương/cơ quan A. 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 3, 4

Hệ thống cung cấp dịch vụ công trực tuyến cấp độ 3, 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.

Lưu ý: Nghiên cứu hướng dẫn tại Điều 8, Điều 9 và các Phụ lục từ 1 đến 5 của Thông tư số 03/2017/TT-BTTTT.

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: Các thuyết minh thành phần

STT	Hệ thống	Cấp độ đề xuất	Nội dung thuyết minh
1	Thuyết minh phương án kỹ thuật đối với hệ thống cổng thông tin nội bộ	1	Phụ lục III.1.
2	Thuyết minh phương án kỹ thuật đối với hệ thống quản lý văn bản	2	Phụ lục III.2.
3	Thuyết minh phương án bảo đảm an toàn thông tin về quản lý	3	Phụ lục III.3.

PHỤ LỤC III.1. 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	Sử dụng tường lửa của hệ điều hành và hệ thống để

Máy chủ	khoản không còn hợp lệ trên máy chủ	cấm các truy cập trái phép tới 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.2. 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 thông tin chuyên ngành 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 **Ứng dụng**	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
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 III.3. 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 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 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 III: CÁC BIỂU MẪU VĂN BẢN

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

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

Kính gửi: (Đơn vị chuyên trách về an toàn thông tin)

(Phòng Văn hóa – Thông tin, đối với chủ quản hệ thống thông tin là UBND cấp huyện; Sở Thông tin và Truyền thông, đối với chủ quản hệ thống thông tin là UBND tỉnh)

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

(Căn cứ các văn bản hướng dẫn thi hành Luật An toàn thông tin mạng và các văn bản liên quan),

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

Phần 1. Thông tin chung

1. Tên hệ thống thông tin:

2. Đơn vị vận hành hệ thống thông tin:

3. Địa chỉ:

4. Cấp độ an toàn hệ thống thông tin đề xuất:

Phần 2. Hồ sơ kèm theo

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

2. Tài liệu thiết kế hệ thống.

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

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

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

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

Kính gửi: (Đơn vị chuyên trách về an toàn thông tin)

(Phòng Văn hóa – Thông tin, đối với chủ quản hệ thống thông tin là UBND cấp huyện; Sở Thông tin và Truyền thông, đối với chủ quản hệ thống thông tin là UBND tỉnh)

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

(Căn cứ các văn bản hướng dẫn thi hành Luật An toàn thông tin mạng và các văn bản liên quan),

(Tên cơ quan, tổ chức) đề nghị (Đơn vị chuyên trách về an toàn thông tin) thẩm định hồ sơ đề xuất cấp độ an toàn hệ thống thông tin:

Phần 1. Thông tin chung

1. Tên hệ thống thông tin:

2. Đơn vị vận hành hệ thống thông tin:

3. Địa chỉ:

4. Cấp độ an toàn hệ thống thông tin đề xuất:

Phần 2. Hồ sơ kèm theo

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

2. Tài liệu thiết kế hệ thống.

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

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

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

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

Kính gửi: Đơn vị chuyên trách về an toàn thông tin
hoặc Sở Thông tin và Truyền thông

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

(Căn cứ các văn bản hướng dẫn thi hành Luật An toàn thông tin mạng và các văn bản liên quan),

(Tên cơ quan, tổ chức) đề nghị Sở Thông tin và Truyền thông cho ý kiến chuyên môn về sự phù hợp của đề xuất cấp độ và phương án bảo đảm an toàn hệ thống thông tin theo cấp độ của hệ thống thông tin:

Phần 1. Thông tin chung

1. Tên hệ thống thông tin:

2. Đơn vị vận hành hệ thống thông tin:

3. Địa chỉ:

4. Cấp độ an toàn hệ thống thông tin đề xuất:

Phần 2. Hồ sơ kèm theo

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

2. Tài liệu thiết kế hệ thống.

Đề nghị Sở Thông tin và Truyền thông xem xét, cho ý kiến./.

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

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

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

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

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

(Căn cứ các văn bản hướng dẫn thi hành Luật An toàn thông tin mạng và các văn bản liên quan),

(Tên cơ quan, tổ chức) đề nghị (Bộ TT&TT/Bộ Quốc phòng/Bộ Công an) thẩm định hồ sơ đề xuất cấp độ an toàn hệ thống thông tin:

Phần 1. Thông tin chung

1. Tên hệ thống thông tin:

2. Đơn vị vận hành hệ thống thông tin:

3. Địa chỉ:

4. Cấp độ an toàn hệ thống thông tin đề xuất:

Phần 2. Hồ sơ kèm theo

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

2. Tài liệu thiết kế hệ thống.

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

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

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

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

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

Kính gửi: Cơ quan chủ quản hệ thống thông tin

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

(Căn cứ các văn bản hướng dẫn thi hành Luật An toàn thông tin mạng và các văn bản liên quan),

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

Phần 1. Thông tin chung

1. Tên hệ thống thông tin:

2. Đơn vị vận hành hệ thống thông tin:

3. Địa chỉ:

4. Cấp độ an toàn hệ thống thông tin đề xuất phê duyệt:

Phần 2. Hồ sơ kèm theo

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

2. Tài liệu thiết kế hệ thống.

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

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

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