BỘ GIÁO DỤC VÀ ĐÀO TẠO
ĐẠI HỌC THÁI NGUYÊN
Số: 5852/QĐ-ĐHTN

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

Thái Nguyên, ngày 04 tháng 12 năm 2023

QUYẾT ĐỊNH

Ban hành Quy định về bảo đảm an toàn hệ thống thông tin theo cấp độ của Đại học Thái Nguyên

GIÁM ĐỐC ĐẠI HỌC THÁI NGUYÊN

Căn cứ Nghị định số 31/CP ngày 04/4/1994 của Chính phủ về việc thành lập Đại học Thái Nguyên;

Căn cứ Thông tư số 10/2020/TT-BGDĐT ngày 14/5/2020 của Bộ trưởng Bộ Giáo dục và Đào tạo ban hành Quy chế tổ chức hoạt động của đại học vùng và các cơ sở giáo dục đại học thành viên;

Căn cứ Nghị quyết số 39/NQ-HĐĐHTN ngày 19 tháng 11 năm 2021 của Hội đồng Đại học Thái Nguyên ban hành Quy chế tổ chức và hoạt động của Đại học Thái Nguyên;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/08/2022 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Theo đề nghị của Giám đốc Trung tâm Số.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy định về bảo đảm an toàn hệ thống thông tin theo cấp độ của Đại học Thái Nguyên.

Điều 2. Quyết định này có hiệu lực kể từ ngày ký.

Điều 3. Chánh Văn phòng, Trưởng các Ban chức năng, Thủ trưởng các đơn vị thành viên, đơn vị thuộc và trực thuộc Đại học Thái Nguyên chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3 (để t/h);
- Lưu: VT, Trung tâm Số.

GIÁM ĐỐC

ĐẠI HỌC THÁI NGUYÊN

PGS.TS. Hoàng Văn Hùng

BỘ GIÁO DỤC VÀ ĐÀO TẠO
ĐẠI HỌC THÁI NGUYÊN

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

QUY ĐỊNH

Bảo đảm an toàn hệ thống thông tin theo cấp độ của Đại học Thái Nguyên
(Ban hành kèm theo Quyết định số 5852/QĐ-ĐHTN ngày 04/12/2023 của Giám đốc Đại học Thái Nguyên)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Văn bản này quy định bảo đảm an toàn hệ thống thông tin theo cấp độ của Đại học Thái Nguyên, bao gồm: xác định hệ thống thông tin và cấp độ an toàn hệ thống thông tin; thẩm quyền, trình tự, thủ tục xác định cấp độ; yêu cầu bảo đảm an toàn hệ thống thông tin theo cấp độ; kiểm tra, đánh giá an toàn thông tin; chế độ báo cáo.

Điều 2. Đối tượng áp dụng

1. Quy định này áp dụng đối với các đơn vị thành viên của Đại học Thái Nguyên trong việc thực hiện xây dựng, thiết lập, quản lý, vận hành, nâng cấp, mở rộng hệ thống thông tin phục vụ ứng dụng công nghệ thông tin trong hoạt động quản lý, đào tạo của đơn vị mình.

2. Khuyến khích các đơn vị thuộc và trực thuộc của Đại học Thái Nguyên áp dụng Quy định này để bảo vệ hệ thống thông tin.

Điều 3. Giải thích từ ngữ

Trong Quy định này, các từ ngữ dưới đây được hiểu như sau:

1. *Xác thực đa nhân tố* là phương pháp xác thực không chỉ dựa vào một mà là kết hợp một số yếu tố liên quan đến người dùng, bao gồm: những thông tin mà người dùng biết (mật khẩu, mã số truy cập, ...), những thông tin mà người dùng sở hữu (chứng thư số, thẻ thông minh, ...) hoặc những thông tin về sinh trắc học của người dùng (vân tay, mống mắt, ...).

2. *Dự phòng nóng* là khả năng thay thế chức năng của thiết bị khi xảy ra sự cố mà không làm gián đoạn hoạt động của hệ thống.

3. *Độ phức tạp cần thiết của mật khẩu* là việc bảo đảm mật khẩu có trên 8 ký tự, trong đó bao gồm cả ký tự chữ cái hoa, chữ cái thường, ký tự đặc biệt và chữ số.

4. *Thiết bị mạng chính hoặc quan trọng* là các thiết bị khi ngừng một phần hay toàn bộ hoạt động mà không có kế hoạch trước sẽ làm gián đoạn hoạt động bình thường của hệ thống thông tin. Thành phần thiết bị mạng chính được xác định theo cấp độ của hệ thống thông tin, bao gồm tối thiểu: thiết bị chuyển mạch trung tâm hoặc tương đương,

thiết bị tường lửa trung tâm, tường lửa ứng dụng web, hệ thống lưu trữ tập trung, tường lửa cơ sở dữ liệu.

Điều 4. Nguyên tắc bảo đảm an toàn hệ thống thông tin theo cấp độ

1. Việc bảo đảm an toàn hệ thống thông tin theo cấp độ trong hoạt động của cơ quan, tổ chức được thực hiện thường xuyên, liên tục từ khâu thiết kế, xây dựng, vận hành đến khi hủy bỏ; tuân thủ theo tiêu chuẩn, quy chuẩn kỹ thuật.

2. Việc bảo đảm an toàn hệ thống thông tin theo cấp độ trong hoạt động của cơ quan, tổ chức được thực hiện một cách tổng thể, đồng bộ, tập trung trong việc đầu tư các giải pháp bảo vệ, có sự dùng chung, chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư thừa, trùng lặp.

3. Việc phân bổ, bố trí nguồn lực để bảo đảm an toàn hệ thống thông tin thực hiện theo thứ tự ưu tiên từ cấp độ cao xuống cấp độ thấp.

Điều 5. Nguyên tắc xác định cấp độ

1. Việc xác định hệ thống thông tin để xác định cấp độ căn cứ trên nguyên tắc như sau:

a) Hệ thống thông tin chỉ có một chủ quản hệ thống thông tin;

b) Hệ thống thông tin có thể hoạt động độc lập, được thiết lập nhằm trực tiếp phục vụ hoặc hỗ trợ hoạt động nghiệp vụ cụ thể của cơ quan, tổ chức thuộc một trong các loại hình hệ thống thông tin quy định tại khoản 2 Điều 8 Quy định này.

2. Trong trường hợp hệ thống thông tin bao gồm nhiều hệ thống thành phần, mỗi hệ thống thành phần lại tương ứng với một cấp độ khác nhau, thì cấp độ hệ thống thông tin được xác định là cấp độ cao nhất trong các cấp độ của các hệ thống thành phần cấu thành.

Chương II
XÁC ĐỊNH HỆ THỐNG THÔNG TIN VÀ CẤP ĐỘ AN TOÀN HỆ THỐNG THÔNG TIN

Điều 6. Chủ quản hệ thống thông tin

1. Chủ quản hệ thống thông tin là một trong các trường hợp sau:

a) Đại học Thái Nguyên;

b) Các đơn vị thành viên và các đơn vị trực thuộc Đại học Thái Nguyên có hệ thống thông tin độc lập;

c) Ngoài 02 trường hợp quy định tại điểm a và điểm b khoản này thì chủ quản hệ thống thông tin 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. Chủ quản hệ thống thông tin có thể ủy quyền cho một tổ chức thay mặt thực hiện quyền quản lý trực tiếp đối với hệ thống thông tin và trách nhiệm bảo đảm an toàn hệ thống thông tin theo quy định tại khoản 2 Điều 22 Quy định này.

Việc ủy quyền phải được thực hiện bằng văn bản, trong đó nêu rõ phạm vi và thời hạn ủy 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.

Điều 7. Đơn vị vận hành hệ thống thông tin

1. Đơn vị vận hành hệ thống thông tin là đơn vị được chủ quản hệ thống thông tin giao nhiệm vụ vận hành hệ thống thông tin. Đơn vị vận hành hệ thống thông tin là một trong các trường hợp sau:

a) Đối với Cơ quan Đại học Thái Nguyên là Văn phòng Đại học Thái Nguyên;

b) Đối với các đơn vị thành viên đơn vị vận hành là các đơn vị chuyên trách được Cơ quan chủ quản giao vận hành hệ thống thông tin;

c) Đối với các đơn vị trực thuộc Đại học Thái Nguyên có hệ thống thông tin độc lập thì đơn vị vận hành là Phòng kỹ thuật hoặc bộ phận được giao nhiệm vụ trực tiếp vận hành hệ thống thông tin.

2. 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.

3. 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.

Điều 8. Phân loại thông tin và hệ thống thông tin

1. Thông tin xử lý thông qua hệ thống thông tin được phân loại theo thuộc tính bí mật như sau:

a) 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;

b) 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;

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

d) 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.

2. Hệ thống thông tin được phân loại theo chức năng phục vụ hoạt động nghiệp vụ như sau:

a) 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 đơn vị;

b) Hệ thống thông tin phục vụ người dùng, tổ chức là hệ thống trực tiếp hoặc hỗ trợ cung cấp dịch vụ trực tuyến, bao gồm các dịch vụ trực tuyến trong giáo dục;

c) Hệ thống cơ sở hạ tầng thông tin là tập hợp trang thiết bị, đường truyền dẫn kết nối phục vụ chung hoạt động của nhiều đơn vị 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;

d) Hệ thống thông tin khác là hệ thống thông tin không thuộc các loại hình trên, được sử dụng để trực tiếp phục vụ hoặc hỗ trợ hoạt động nghiệp vụ phục vụ đào tạo cụ thể của các đơn vị thành viên và các đơn vị trực thuộc.

Điều 9. Tiêu chí xác định cấp độ 1

Hệ thống thông tin cấp độ 1 là hệ thống thông tin phục vụ hoạt động nội bộ của đơn vị và chỉ xử lý thông tin công cộng.

Điều 10. Tiêu chí xác định cấp độ 2

Hệ thống thông tin cấp độ 2 là hệ thống thông tin có một trong các tiêu chí cụ thể như sau:

1. Hệ thống thông tin phục vụ hoạt động nội bộ của đơn vị và có xử lý thông tin riêng, thông tin cá nhân của người sử dụng nhưng không xử lý thông tin bí mật nhà nước.

2. Hệ thống thông tin phục người dùng thuộc một trong các loại hình như sau:

a) Cung cấp dịch vụ trực tuyến không thuộc danh mục dịch vụ kinh doanh có điều kiện;

b) Cung cấp dịch vụ trực tuyến khác có xử lý thông tin riêng, thông tin cá nhân của dưới 10.000 người sử dụng.

3. Hệ thống cơ sở hạ tầng thông tin phục vụ hoạt động của một đơn vị.

Điều 11. Tiêu chí xác định cấp độ 3

Hệ thống thông tin cấp độ 3 là hệ thống thông tin có một trong các tiêu chí cụ thể như sau:

1. Hệ thống thông tin xử lý thông tin bí mật nhà nước hoặc hệ thống phục vụ quốc phòng, an ninh khi bị phá hoại sẽ làm tổn hại tới quốc phòng, an ninh quốc gia.

2. Hệ thống thông tin phục vụ người dùng thuộc một trong các loại hình như sau:

a) Cung cấp dịch vụ trực tuyến thuộc danh mục dịch vụ kinh doanh có điều kiện;

b) Cung cấp dịch vụ trực tuyến khác có xử lý thông tin riêng, thông tin cá nhân của từ 10.000 người sử dụng trở lên.

3. Hệ thống cơ sở hạ tầng thông tin dùng chung phục vụ hoạt động của các đơn vị trong phạm vi Đại học Thái Nguyên.

Chương III
THẨM QUYỀN, TRÌNH TỰ, THỦ TỤC XÁC ĐỊNH CẤP ĐỘ

Điều 12. Thẩm quyền thẩm định và phê duyệt cấp độ

1. Đối với hệ thống thông tin được đề xuất là cấp độ 1 hoặc cấp độ 2:

Trung tâm Số – Đại học Thái Nguyên 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.

2. Đối với hệ thống thông tin được đề xuất là cấp độ 3:

a) Trung tâm Số – Đại học Thái Nguyên thực hiện thẩm định hồ sơ đề xuất cấp độ;

b) Đại học Thái Nguyên phê duyệt hồ sơ đề xuất cấp độ.

Điều 13. Trình tự, thủ tục xác định cấp độ đối với dự án đầu tư xây dựng mới hoặc mở rộng, nâng cấp hệ thống thông tin

1. Chủ đầu tư xây dựng 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 và quy định Quy định này.

2. 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 và quy định của Quy định này.

3. Tài liệu thuyết minh đề xuất cấp độ theo quy định tại Điều 15 Quy định này.

Điều 14. Trình tự, thủ tục xác định cấp độ đối với hệ thống thông tin đang vận hành

1. Lập hồ sơ đề xuất cấp độ:

a) Đơn vị vận hành hệ thống thông tin lập hồ sơ đề xuất cấp độ theo quy định tại Điều 15 Quy định này;

b) Đối với hệ thống thông tin được đề xuất là cấp độ 1 hoặc cấp độ 2:

Đơn vị vận hành hệ thống thông tin gửi hồ sơ đề xuất cấp độ tới đơn vị thẩm định để thực hiện thẩm định theo quy định tại khoản 1 Điều 12 Quy định này;

c) Đối với hệ thống thông tin được đề xuất là cấp độ 3:

Đơn vị vận hành hệ thống thông tin gửi hồ sơ đề xuất cấp độ tới đơn vị thẩm định để thực hiện thẩm định theo quy định tại điểm a khoản 2 Điều 12 Quy định này;

2. Thẩm định hồ sơ đề xuất cấp độ:

Đơn vị có thẩm quyền thực hiện thẩm định hồ sơ đề xuất cấp độ theo quy định tại Điều 17 Quy định này.

3. Phê duyệt đề xuất cấp độ:

a) Đối với hệ thống thông tin được đề xuất là cấp độ 1 hoặc cấp độ 2:

Đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin phê duyệt đề xuất cấp độ, gửi báo cáo chủ quản hệ thống thông tin;

b) Đối với hệ thống thông tin được đề xuất là cấp độ 3:

Đơn vị vận hành hệ thống thông tin trình chủ quản hệ thống thông tin phê duyệt đề xuất cấp độ.

Điều 15. Hồ sơ đề xuất cấp độ

Hồ sơ đề xuất cấp độ bao gồm:

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

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

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

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

3. Tài liệu thuyết minh về việc đề xuất cấp độ theo quy định tại Điều 16 Quy định này.

4. Tài liệu thuyết minh phương án bảo đảm an toàn thông tin theo cấp độ tương ứng theo quy định tại Điều 16 Quy định này.

Điều 16. Thuyết minh cấp độ an toàn hệ thống thông tin

1. Đối với hệ thống thông tin được đầu tư xây dựng mới hoặc mở rộng, nâng cấp, tùy thuộc vào hình thức đầu tư, phương án kỹ thuật trong Báo cáo kinh tế - kỹ thuật (trường hợp dự án đầu tư áp dụng phương án thiết kế 01 bước), trong Thiết kế cơ sở thuộc Báo cáo nghiên cứu khả thi (trường hợp dự án đầu tư áp dụng phương án thiết kế 02 bước), trong Kế hoạch thuê dịch vụ công nghệ thông tin (trong trường hợp thuê dịch vụ công nghệ thông tin) hoặc trong Đề cương và dự toán chi tiết (trong trường hợp đầu tư ứng dụng công nghệ thông tin không phải lập dự án) phải đáp ứng các yêu cầu của phương án bảo đảm an toàn thông tin theo cấp độ được đề xuất, được thuyết minh trong Hồ sơ đề xuất cấp độ.

2. Thuyết minh Hồ sơ đề xuất cấp độ, bao gồm các thành phần sau đây:

a) Thuyết minh tổng quan về hệ thống thông tin;

b) Thuyết minh về việc đề xuất cấp độ;

c) Thuyết minh phương án bảo đảm an toàn thông tin.

3. Thuyết minh tổng quan về hệ thống thông tin, bao gồm các nội dung:

a) Thông tin về chủ quản hệ thống thông tin, gồm: tên chủ quản hệ thống thông tin; quy định chức năng, nhiệm vụ và quyền hạn; người đại diện, chức vụ; địa chỉ; thông tin liên hệ (bao gồm số điện thoại, thư điện tử);

b) Thông tin về đơn vị vận hành hệ thống thông tin, gồm: tên đơn vị vận hành; quy định chức năng, nhiệm vụ và quyền hạn; người đại diện, chức vụ; địa chỉ; thông tin liên hệ (bao gồm số điện thoại, thư điện tử);

c) Mô tả phạm vi, quy mô của hệ thống thông tin, trong đó cần làm rõ phạm vi của hệ thống, quy mô của hệ thống và đối tượng phục vụ của hệ thống;

d) Mô tả hiện trạng kiến trúc hệ thống (đối với hệ thống đang vận hành) hoặc mô tả kiến trúc hệ thống (đối với hệ thống được xây dựng mới hoặc nâng cấp, mở rộng), trong đó mô tả cụ thể mô hình lô-gic, mô hình vật lý của hệ thống, danh mục thiết bị và thiết bị mạng chính trong hệ thống (bao gồm tên thiết bị/chủng loại, vị trí triển khai, mục đích sử dụng), danh mục ứng dụng/dịch vụ cung cấp bởi hệ thống (bao gồm tên dịch vụ, máy chủ triển khai/vị trí triển khai/hệ điều hành máy chủ, mục đích sử dụng dịch vụ), quy hoạch các vùng mạng và địa chỉ IP trong hệ thống (bao gồm vùng mạng, địa chỉ IP nội bộ (IP Private), địa chỉ IP công khai (IP Public)).

4. Thuyết minh về việc đề xuất cấp độ, bao gồm các nội dung:

a) Danh mục các hệ thống thông tin và cấp độ tương ứng, bao gồm: tên hệ thống thông tin, cấp độ đề xuất, căn cứ đề xuất đối với từng hệ thống thông tin;

b) Thuyết minh chi tiết đối với các hệ thống thông tin, trong đó cần làm rõ loại thông tin được xử lý, loại hệ thống thông tin, căn cứ đề xuất cấp độ đối với từng hệ thống thông tin.

5. Thuyết minh phương án bảo đảm an toàn thông tin, bao gồm các nội dung:

a) Thuyết minh phương án đáp ứng các yêu cầu về quản lý tương ứng với cấp độ đề xuất;

b) Thuyết minh phương án đáp ứng các yêu cầu về kỹ thuật tương ứng với cấp độ đề xuất.

Điều 17. Thẩm định hồ sơ đề xuất cấp độ

1. Nội dung thẩm định hồ sơ đề xuất cấp độ:

a) Sự phù hợp về việc đề xuất cấp độ;

b) Sự phù hợp của phương án bảo đảm an toàn hệ thống thông tin trong thiết kế sơ bộ, thiết kế thi công hoặc tài liệu có giá trị tương đương theo cấp độ tương ứng;

c) Sự phù hợp của phương án bảo đảm an toàn hệ thống thông tin trong quá trình vận hành hệ thống theo cấp độ tương ứng.

2. Trường hợp đơn vị chuyên trách về an toàn thông tin, đồng thời được chủ quản hệ thống thông tin giao quản lý, vận hành hệ thống thông tin, việc tổ chức thẩm định Hồ sơ đề xuất cấp độ được thực hiện theo một trong các phương án sau đây:

a) Đơn vị chuyên trách về an toàn thông tin trình chủ quản hệ thống thông tin giao một đơn vị trực thuộc có đủ năng lực chủ trì, tổ chức thẩm định.

b) Đơn vị chuyên trách về an toàn thông tin trình chủ quản hệ thống thông tin thành lập Hội đồng thẩm định độc lập thực hiện nhiệm vụ thẩm định Hồ sơ đề xuất cấp độ.

3. Thời gian thẩm định hồ sơ xác định cấp độ:

Đối với hệ thống thông tin đề xuất cấp độ 3, thời gian thẩm định tối đa là 15 ngày kể từ ngày nhận đủ hồ sơ hợp lệ;

Điều 18. Hồ sơ phê duyệt đề xuất cấp độ

1. Hồ sơ phê duyệt đề xuất cấp độ bao gồm:

a) Hồ sơ đề xuất cấp độ;

b) Ý kiến thẩm định của cơ quan chủ trì thẩm định đối với hệ thống thông tin đề xuất từ cấp độ 3 trở lên.

2. Thời gian xử lý hồ sơ phê duyệt cấp độ:

Thời gian xử lý tối đa là 07 ngày làm việc kể từ ngày nhận đủ hồ sơ hợp lệ.

Điều 19. Trình tự, thủ tục xác định lại cấp độ đối với hệ thống thông tin đã được phê duyệt cấp độ

Đối với hệ thống thông tin đã được phê duyệt cấp độ, trong trường hợp phải xác định lại cấp độ cho phù hợp với tình hình thực tế thì thực hiện theo trình tự, thủ tục xác định lần đầu.

Chương IV
YÊU CẦU BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN THEO CẤP ĐỘ

Điều 20. Yêu cầu chung

1. Việc bảo đảm an toàn hệ thống thông tin theo cấp độ thực hiện theo yêu cầu cơ bản quy định tại Quy định này và Tiêu chuẩn quốc gia TCVN 11930:2017 về Công nghệ thông tin - các kỹ thuật an toàn - yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ.

2. Yêu cầu cơ bản đối với từng cấp độ quy định tại Quy định này là yêu cầu tối thiểu để bảo đảm an toàn hệ thống thông tin và không bao gồm các yêu cầu bảo đảm an toàn vật lý.

3. Yêu cầu cơ bản về quản lý, bao gồm:

a) Thiết lập chính sách an toàn thông tin;

b) Tổ chức bảo đảm an toàn thông tin;

c) Bảo đảm nguồn nhân lực;

d) Quản lý thiết kế, xây dựng hệ thống;

đ) Quản lý vận hành hệ thống;

e) Phương án Quản lý rủi ro an toàn thông tin;

g) Phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin.

4. Yêu cầu cơ bản về kỹ thuật, bao gồm:

a) Bảo đảm an toàn mạng;

b) Bảo đảm an toàn máy chủ;

c) Bảo đảm an toàn ứng dụng;

d) Bảo đảm an toàn dữ liệu.

5. Việc xây dựng phương án bảo đảm an toàn thông tin đáp ứng yêu cầu cơ bản theo từng cấp độ thực hiện theo nguyên tắc quy định tại khoản 2 Điều 4 Nghị định số 85/2016/NĐ-CP, cụ thể như sau:

Đối với hệ thống thông tin cấp độ 1, 2, 3: Phương án bảo đảm an toàn thông tin phải xem xét khả năng dùng chung giữa các hệ thống thông tin đối với các giải pháp bảo vệ, chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư thừa, trùng lặp, lãng phí. Trong trường hợp đầu tư mới, phải có thuyết minh về việc giải pháp đã có không đáp ứng được yêu cầu cơ bản.

6. Hệ thống thông tin khi được đầu tư xây dựng mới hoặc mở rộng, nâng cấp phải triển khai đầy đủ phương án bảo đảm an toàn thông tin đã được phê duyệt tại Hồ sơ đề xuất cấp độ và đáp ứng các yêu cầu an toàn tại Điều 20 và Điều 21 tại Quy định này này trước khi đưa vào vận hành, khai thác.

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

8. Yêu cầu bảo đảm an toàn thông tin đối với phần mềm nội bộ khi xây dựng mới hoặc mở rộng, nâng cấp:

a) Phần mềm nội bộ được xây dựng mới hoặc mở rộng, nâng cấp phải tuân thủ Khung phát triển phần mềm an toàn;

b) Đáp ứng yêu cầu an toàn cơ bản đối với Phần mềm nội bộ.

9. Trường hợp hệ thống thông tin cấp độ 3 được triển khai dưới hình thức thuê dịch vụ công nghệ thông tin tại Trung tâm dữ liệu hoặc Điện toán đám mây, thiết kế hệ thống phải đáp ứng các yêu cầu sau:

a) Phải được thiết kế tách riêng, độc lập với các hệ thống khác về lô-gic và có biện pháp quản lý truy cập giữa các hệ thống;

b) Các vùng mạng trong hệ thống phải được thiết kế tách riêng, độc lập với nhau về lô-gic và có biện pháp quản lý truy cập giữa các vùng mạng;

c) Có phân vùng lưu trữ được phân tách độc lập về lô-gic.

Điều 21. Phương án bảo đảm an toàn thông tin đối với từng cấp độ

1. Phương án bảo đảm an toàn hệ thống thông tin cấp độ 1 phải đáp ứng yêu cầu quy định chi tiết tại Phụ lục I ban hành kèm theo Quy định này.

2. Phương án bảo đảm an toàn hệ thống thông tin cấp độ 2 phải đáp ứng yêu cầu như đối với cấp độ 1 và bổ sung yêu cầu quy định chi tiết tại Phụ lục II ban hành kèm theo Quy định này.

3. Phương án bảo đảm an toàn hệ thống thông tin cấp độ 3 phải đáp ứng yêu cầu như đối với cấp độ 2 và bổ sung yêu cầu quy định chi tiết tại Phụ lục III ban hành kèm theo Quy định này.

4. Các mẫu văn bản xác định cấp độ an toàn hệ thống thông tin quy định chi tiết tại Phụ lục 4 ban hành kèm theo Quy định này.

Điều 22. Trách nhiệm của chủ quản hệ thống thông tin

1. Người đứng đầu các đơn vị là chủ quản hệ thống thông tin có trách nhiệm:

a) Trực tiếp chỉ đạo và phụ trách công tác bảo đảm an toàn thông tin trong hoạt động của đơn vị mình;

b) 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;

- 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.

2. Chủ quản hệ thống thông tin có trách nhiệm:

a) Chỉ đạo đơn vị vận hành hệ thống thông tin lập hồ sơ đề xuất cấp độ theo Quy định này;

b) Chỉ đạo, tổ chức thực hiện phương án bảo đảm an toàn hệ thống thông tin theo cấp độ đối với hệ thống thông tin thuộc phạm vi mình quản lý theo quy định tại Điều 25, 26 và 27 của Luật an toàn thông tin mạng, Quy định này và quy định của pháp luật liên quan;

c) Chỉ đạo, tổ chức thực hiện kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin trong phạm vi đơn vị mình, cụ thể như sau:

- Định kỳ 02 năm thực hiện kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin tổng thể trong hoạt động của cơ quan, tổ chức mình;

- Định kỳ hàng năm thực hiện kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin đối với hệ thống cấp độ 3;

- Việc kiểm tra, đánh giá an toàn thông tin và đánh giá rủi ro an toàn thông tin đối với hệ thống từ cấp độ 3 phải do tổ chức chuyên môn được cơ quan có thẩm quyền cấp phép; tổ chức sự nghiệp nhà nước có chức năng, nhiệm vụ phù hợp hoặc do tổ chức chuyên môn được cấp có thẩm quyền chỉ định thực hiện.

d) Chỉ đạo, tổ chức thực hiện đào tạo ngắn hạn, tuyên truyền, phổ biến, nâng cao nhận thức và diễn tập về an toàn thông tin, cụ thể như sau:

- Đào tạo, bồi dưỡng theo các chương trình đào tạo ngắn hạn nâng cao kiến thức, kỹ năng về an toàn thông tin cho cán bộ, viên chức, người lao động làm về an toàn thông tin trong đơn vị mình;

- Tuyên truyền, phổ biến nâng cao nhận thức về an toàn thông tin cho cán bộ, viên chức, người lao động trong đơn vị mình;

- Diễn tập bảo đảm an toàn thông tin trong hoạt động của đơn vị mình; Tham gia đào tạo bồi dưỡng theo các trương trình đào tạo ngắn hạn nâng cao kiến thức, kỹ năng về an toàn thông tin do Đại học Thái Nguyên tổ chức.

đ) Chỉ đạo đơn vị vận hành hệ thống thông tin phối hợp với Trung tâm Số - Đại học Thái Nguyên trong việc xử lý, giảm thiểu tấn công mạng, hỗ trợ giám sát an toàn thông tin cho hệ thống thông tin cung cấp dịch vụ trực tuyến, phát triển đại học điện tử.

Điều 23. Trách nhiệm của đơn vị vận hành hệ thống thông tin

1. Thực hiện xác định cấp độ an toàn hệ thống thông tin theo quy định tại Điều 14 Quy định này.

2. Thực hiện bảo vệ hệ thống thông tin theo quy định của pháp luật và hướng dẫn, tiêu chuẩn, quy chuẩn an toàn thông tin.

3. Định kỳ đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin, báo cáo chủ quản hệ thống thông tin điều chỉnh nếu cần thiết.

4. Định kỳ hoặc đột xuất báo cáo công tác thực thi bảo đảm an toàn hệ thống thông tin theo yêu cầu của chủ quản hệ thống thông tin hoặc yêu cầu của Đại học Thái Nguyên.

5. Phối hợp, thực hiện theo yêu cầu của cơ quan chức năng liên quan của Đại học Thái Nguyên trong công tác bảo đảm an toàn thông tin.

Điều 24. Trách nhiệm của Trung tâm Số

1. Tham mưu, tổ chức thực thi, đôn đốc, kiểm tra, giám sát công tác bảo đảm an toàn thông tin.

2. Thẩm định, phê duyệt hoặc cho ý kiến về mặt chuyên môn đối với hồ sơ đề xuất cấp độ theo thẩm quyền quy định tại Điều 12 Quy định này.

Điều 25. Trách nhiệm của Đại học Thái Nguyên

Thực hiện phê duyệt hồ sơ đề xuất cấp độ theo thẩm quyền quy định tại điểm b khoản 2 Điều 15 Quy định này.

Điều 26. Kinh phí bảo đảm an toàn thông tin

Kinh phí thực hiện bảo đảm an toàn thông tin thực hiện theo quy định của pháp luật hiện hành.

Chương V
KIỂM TRA, ĐÁNH GIÁ AN TOÀN THÔNG TIN

Điều 27. Quy định chung về hoạt động kiểm tra, đánh giá

1. Nội dung kiểm tra, đánh giá:

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

b) Kiểm tra, đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin theo phương án bảo đảm an toàn thông tin được phê duyệt;

c) Kiểm tra, đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thông tin.

2. Tần suất kiểm tra, đánh giá:

a) Kiểm tra, đánh giá định kỳ theo quy định tại điểm c khoản 2 Điều 20 Nghị định 85/2016/NĐ-CP;

b) Kiểm tra, đánh giá đột xuất theo yêu cầu của cấp có thẩm quyền.

3. Hình thức kiểm tra, đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thông tin, gồm 03 hình thức sau:

a) Kiểm tra, đánh giá hộp đen (Black box);

b) Kiểm tra, đánh giá hộp xám (Gray box);

c) Kiểm tra, đánh giá hộp trắng (White box).

4. Cấp có thẩm quyền yêu cầu kiểm tra, đánh giá:

a) Giám đốc Đại học Thái Nguyên;

b) Chủ quản hệ thống thông tin đối với hệ thống thông tin thuộc thẩm quyền quản lý;

c) Trung tâm Số – Đại học Thái Nguyên đối với hệ thống thông tin do đơn vị này phê duyệt hồ sơ đề xuất cấp độ.

5. 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.

6. 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 28. Nội dung kiểm tra, đánh giá về an toàn thông tin

1. Nội dung kiểm tra, đánh giá việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ, bao gồm:

a) Kiểm tra, đánh giá tuân thủ đối với Chủ quản hệ thống thông tin theo quy định tại Điều 20 Nghị định 85/2016/NĐ-CP, bao gồm: việc thực hiện thành lập/chỉ định đơn vị chuyên trách/bộ phận chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin theo quy định tại khoản 1 Điều 20 Nghị định 85/2016/NĐ-CP; việc thực hiện lập Hồ sơ đề xuất cấp độ, tổ chức thẩm định, phê duyệt Hồ sơ đề xuất cấp độ theo quy định đối với các hệ thống thông tin thuộc phạm vi quản lý; việc triển khai phương án bảo đảm an toàn thông tin theo phương án trong Hồ sơ đề xuất cấp độ được phê duyệt đối với các hệ thống thông tin thuộc phạm vi quản lý; việc tổ chức thực hiện kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin trong phạm vi cơ quan, tổ chức mình theo quy định tại điểm c khoản 2 Điều 20 Nghị định 85/2016/NĐ-CP; việc tổ chức thực

hiện đào tạo ngắn hạn, tuyên truyền, phổ biến, nâng cao nhận thức và diễn tập về an toàn thông tin theo quy định tại điểm d Khoản 2 Điều 20 Nghị định 85/2016/NĐ-CP;

b) Kiểm tra, đánh giá tuân thủ đối với Đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin theo quy định tại Điều 21 Nghị định 85/2016/NĐ-CP, bao gồm các nội dung: công tác tham mưu, tổ chức thực thi, đôn đốc, kiểm tra, giám sát công tác bảo đảm an toàn thông tin; công tác thẩm định, phê duyệt hoặc cho ý kiến về mặt chuyên môn đối với Hồ sơ đề xuất cấp độ theo thẩm quyền quy định;

c) Kiểm tra, đánh giá tuân thủ đối với Đơn vị vận hành theo quy định tại Điều 22 Nghị định 85/2016/NĐ-CP;

d) Kiểm tra, đánh giá việc tổ chức thực thi các biện pháp bảo đảm an toàn thông tin theo phương án bảo đảm an toàn thông tin được phê duyệt.

2. Nội dung kiểm tra, đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin theo phương án bảo đảm an toàn thông tin được phê duyệt, bao gồm:

a) Kiểm tra tính đầy đủ và phù hợp của Quy chế bảo đảm an toàn thông tin theo phương án bảo đảm an toàn thông tin về quản lý được phê duyệt;

b) Đánh giá việc tuân thủ các quy định, quy trình trong Quy chế bảo đảm an toàn thông tin trong quá trình vận hành, khai thác, kết thúc hoặc hủy bỏ hệ thống thông tin;

c) Đánh giá việc thiết kế hệ thống theo phương án bảo đảm an toàn thông tin được phê duyệt;

d) Đánh giá việc thiết lập, cấu hình hệ thống theo phương án bảo đảm an toàn thông tin được phê duyệt;

đ) Kiểm tra việc cấu hình, tăng cường bảo mật cho thiết bị hệ thống, hệ điều hành, ứng dụng, cơ sở dữ liệu và các thành phần khác liên quan trong hệ thống theo hướng dẫn của Bộ Thông tin và Truyền thông.

3. Nội dung kiểm tra, đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thông tin, bao gồm:

a) Dò quét, phát hiện mã độc, lỗ hổng, điểm yếu của hệ thống, thử nghiệm tấn công xâm nhập đối với các thiết bị hệ thống, hệ điều hành, ứng dụng, cơ sở dữ liệu và các thành phần khác liên quan trong hệ thống;

b) Đánh giá an toàn mã nguồn đối với phần mềm nội bộ;

c) Đưa ra phương án và kế hoạch xử lý lỗ hổng, điểm yếu và phương án cấu hình, tăng cường bảo mật đối với các nội dung kiểm tra được đánh giá là chưa đạt.

Chương VI
CHẾ ĐỘ BÁO CÁO

Điều 29. Quy định chung về chế độ báo cáo

1. Phương thức gửi, nhận báo cáo:

a) Gửi qua hệ thống quản lý văn bản và điều hành;

b) Gửi qua hệ thống thư điện tử;

c) Các phương thức khác theo quy định của pháp luật.

2. Tần suất thực hiện báo cáo:

a) Định kỳ hàng năm;

b) Đột xuất theo đề nghị của cơ quan có thẩm quyền.

3. Thời gian chốt số liệu báo cáo định kỳ hàng năm:

Tính từ ngày 15 tháng 12 năm trước kỳ báo cáo đến ngày 14 tháng 12 của kỳ báo cáo.

4. Thời hạn gửi báo cáo đối với báo cáo định kỳ hàng năm:

a) Đơn vị chuyên trách về an toàn thông tin, đơn vị vận hành hệ thống thông tin gửi báo cáo tới chủ quản hệ thống thông tin trước ngày 20 tháng 12 hàng năm;

b) Chủ quản hệ thống thông tin gửi báo cáo Đại học Thái Nguyên trước ngày 25 tháng 12 hàng năm.

Điều 30. Nội dung báo cáo

1. Thông tin chung về chủ quản hệ thống thông tin, đơn vị chuyên trách về an toàn thông tin, đơn vị vận hành đối với từng hệ thống thông tin thuộc phạm vi quản lý, gồm: tên chủ quản hệ thống thông tin, đơn vị chuyên trách an toàn thông tin, đơn vị vận hành; quy định chức năng, nhiệm vụ và quyền hạn; người đại diện, chức vụ; địa chỉ; thông tin liên hệ (bao gồm số điện thoại, thư điện tử).

2. Danh sách các hệ thống thông tin thuộc phạm vi quản lý, gồm: tên hệ thống, đơn vị vận hành, cấp độ đề xuất.

3. Danh sách hệ thống thông tin được phê duyệt Hồ sơ đề xuất cấp độ theo quy định.

4. Danh sách hệ thống thông tin đã triển khai đầy đủ, mới triển khai một phần hoặc chưa triển khai các biện pháp bảo vệ đáp ứng các yêu cầu an toàn theo phương án bảo đảm an toàn thông tin theo cấp độ đã được phê duyệt.

5. Danh sách hệ thống thông tin có Quy chế bảo đảm an toàn thông tin theo quy định.

6. Danh sách hệ thống thông tin tuân thủ các quy định, quy trình trong Quy chế bảo đảm an toàn thông tin trong quá trình vận hành, khai thác, kết thúc hoặc hủy bỏ hệ thống thông tin.

7. Danh sách hệ thống thông tin được kiểm tra, đánh giá theo quy định.

8. Đánh giá về việc triển khai các biện pháp bảo đảm an toàn thông tin theo phương án bảo đảm an toàn thông tin được phê duyệt trong Hồ sơ đề xuất cấp độ theo từng tiêu chí, yêu cầu.

9. Thông tin Quyết định phê duyệt Hồ sơ đề xuất cấp độ, phương án bảo đảm an toàn thông tin được phê duyệt trong Hồ sơ đề xuất cấp độ theo từng tiêu chí, yêu cầu (đã

đáp ứng đầy đủ/chưa đáp ứng đầy đủ; kế hoạch hoặc lộ trình hoàn thiện tiêu chí, yêu cầu chưa đáp ứng).

10. Thông tin Quyết định ban hành và Quy chế bảo đảm an toàn thông tin.

11. Các thông tin khác theo yêu cầu của cơ quan có thẩm quyền.

Chương IX
TỔ CHỨC THỰC HIỆN

Điều 31. Trách nhiệm thi hành

1. Đối với Đại học Thái Nguyên

Giao Trung tâm Số chủ trì, phối hợp với Văn phòng, các ban chức năng hướng dẫn, theo dõi việc thực hiện Quy định này.

2. Đối với các đơn vị

Thủ trưởng các đơn vị thành viên, đơn vị trực thuộc có trách nhiệm tổ chức triển khai thực hiện Quy định này tại đơn vị mình.

Điều 32. Quy định về sửa đổi, bổ sung

1. Trường hợp các văn bản dẫn chiếu tại Quy định này được sửa đổi, bổ sung hoặc thay thế thì thực hiện theo các văn bản mới đó.

2. Trong quá trình thực hiện Quy định này, nếu có vướng mắc, các cá nhân, cơ quan, đơn vị liên hệ với Đại học Thái Nguyên (qua Trung tâm Số) để xem xét, quyết định sửa đổi, bổ sung cho phù hợp./.

Phụ lục I

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

(Ban hành kèm theo Quyết định số /QĐ-ĐHTN ngày ....tháng.....năm 2023 của Giám đốc Đại học Thái Nguyên)

I. YÊU CẦU QUẢN LÝ

STT	Yêu cầu	TCVN 11930:2017
1.1	**Thiết lập chính sách an toàn thông tin**	**Mục 5.1.1**
1.1.1	Chính sách an toàn thông tin	Mục 5.1.1.1
1.1.2	Xây dựng và công bố	Mục 5.1.1.2
1.1.3	Rà soát, sửa đổi	Mục 5.1.1.3
1.2	**Tổ chức bảo đảm an toàn thông tin**	**Mục 5.1.2**
1.2.1	Đơn vị chuyên trách về an toàn thông tin	Mục 5.1.2.1
1.2.2	Phối hợp với cơ quan/tổ chức có thẩm quyền	Mục 5.1.2.2
1.3	**Bảo đảm nguồn nhân lực**	**Mục 5.1.3**
1.3.1	Tuyển dụng	Mục 5.1.3.1
1.3.2	Trong quá trình làm việc	Mục 5.1.3.2
1.3.3	Chấm dứt hoặc thay đổi công việc	Mục 5.1.3.3
1.4	**Quản lý thiết kế, xây dựng hệ thống**	**Mục 5.1.4**
1.4.1	Thiết kế an toàn hệ thống thông tin	Mục 5.1.4.1
1.4.2	Thử nghiệm và nghiệm thu hệ thống	Mục 5.1.4.2
1.5	**Quản lý vận hành hệ thống**	**Mục 5.1.5**
1.5.1	Quản lý an toàn mạng	Mục 5.1.5.1
1.5.2	Quản lý an toàn máy chủ và ứng dụng	Mục 5.1.5.2
1.5.3	Quản lý an toàn dữ liệu	Mục 5.1.5.3
1.6	**Phương án Quản lý rủi ro an toàn thông tin**	
1.7	**Phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ**	

II. YÊU CẦU KỸ THUẬT

1. Yêu cầu về thiết kế hệ thống

a) Thiết kế các vùng mạng trong hệ thống theo chức năng, các vùng mạng tối thiểu bao gồm:

i. Vùng mạng nội bộ;

ii. Vùng mạng biên;

iii. Vùng DMZ.

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

i. Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn sử dụng mạng riêng ảo hoặc phương án tương đương;

ii. Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập, sử dụng sản phẩm Tường lửa có tích hợp chức năng phòng, chống xâm nhập hoặc phương án tương đương;

iii. Có phương án phòng chống mã độc cho máy chủ và máy trạm sử dụng sản phẩm Phòng chống mã độc hoặc phương án tương đương.

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

STT	Yêu cầu	TCVN 11930:2017
1.1	**Bảo đảm an toàn mạng**	**Mục 5.2.1**
1.1.1	Kiểm soát truy cập từ bên ngoài mạng	Mục 5.2.1.2
1.1.2	Nhật kí hệ thống	Mục 5.2.1.3
1.1.3	Phòng chống xâm nhập	Mục 5.2.1.4
1.1.4	Bảo vệ thiết bị hệ thống	Mục 5.2.1.5
1.2	**Bảo đảm an toàn máy chủ**	**Mục 5.2.2**
1.2.1	Xác thực	Mục 5.2.2.1
1.2.2	Kiểm soát truy cập	Mục 5.2.2.2
1.2.3	Nhật ký hệ thống	Mục 5.2.2.3
1.2.4	Phòng chống xâm nhập	Mục 5.2.2.4
1.2.5	Phòng chống phần mềm độc hại	Mục 5.2.2.5
1.3	**Bảo đảm an toàn ứng dụng**	**Mục 5.2.3**
1.3.1	Xác thực	Mục 5.2.3.1
1.3.2	Kiểm soát truy cập	Mục 5.2.3.2
1.3.3	Nhật kí hệ thống	Mục 5.2.3.3
1.4	**Bảo đảm an toàn dữ liệu**	**Mục 5.2.4**
1.4.1	Sao lưu dự phòng	Mục 5.2.4.1

Phụ lục II

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

(Ban hành kèm theo Quyết định số /QĐ-ĐHTN ngày ....tháng.....năm 2023 của Giám đốc Đại học Thái Nguyên)

I. YÊU CẦU QUẢN LÝ

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

1.6	**Phương án Quản lý rủi ro an toàn thông tin**
1.7	**Phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ**

II. YÊU CẦU KỸ THUẬT

1. Yêu cầu về thiết kế hệ thống

a) Thiết kế các vùng mạng trong hệ thống theo chức năng, các vùng mạng tối thiểu bao gồm:

i. Vùng mạng nội bộ;

ii. Vùng mạng biên;

iii. Vùng DMZ;

iv. Vùng máy chủ nội bộ;

v. Vùng mạng không dây (nếu có) tách riêng, độc lập với các vùng mạng khác.

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

i. Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn sử dụng mạng riêng ảo hoặc phương án tương đương;

ii. Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập, sử dụng sản phẩm Tường lửa có tích hợp chức năng phòng, chống xâm nhập hoặc phương án tương đương;

iii. Có phương án phòng chống mã độc cho máy chủ và máy trạm sử dụng sản phẩm Phòng chống mã độc hoặc phương án tương đương;

iv. Có phương án phòng chống tấn công mạng cho ứng dụng web; sử dụng sản phẩm Tường lửa ứng dụng web đối với hệ thống thông tin theo quy định tại khoản 2 Điều 8 Nghị định 85/2016/NĐ-CP ;

v. Có phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử đối với hệ thống thư điện tử;

vi. Có phương án dự phòng cho các thiết bị mạng chính, bao gồm thiết bị chuyển mạch trung tâm hoặc tương đương, thiết bị tường lửa trung tâm.

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

STT	Yêu cầu	TCVN 11930:2017
1.1	**Bảo đảm an toàn mạng**	**Mục 6.2.1**
1.1.1	Kiểm soát truy cập từ bên ngoài mạng	Mục 6.2.1.2
1.1.2	Kiểm soát truy cập từ bên trong mạng	Mục 6.2.1.3
1.1.3	Nhật kí hệ thống	Mục 6.2.1.4
1.1.4	Phòng chống xâm nhập	Mục 6.2.1.5

1.1.5	Bảo vệ thiết bị hệ thống	Mục 6.2.1.6
1.2	**Bảo đảm an toàn máy chủ**	**Mục 6.2.2**
1.2.1	Xác thực	Mục 6.2.2.1
1.2.2	Kiểm soát truy cập	Mục 6.2.2.2
1.2.3	Nhật ký hệ thống	Mục 6.2.2.3
1.2.4	Phòng chống xâm nhập	Mục 6.2.2.4
1.2.5	Phòng chống phần mềm độc hại	Mục 6.2.2.5
1.2.6	Xử lý máy chủ khi chuyển giao	Mục 6.2.2.6
1.3	**Bảo đảm an toàn ứng dụng**	**Mục 6.2.3**
1.3.1	Xác thực	Mục 6.2.3.1
1.3.2	Kiểm soát truy cập	Mục 6.2.3.2
1.3.3	Nhật kí hệ thống	Mục 6.2.3.3
1.3.4	An toàn ứng dụng và mã nguồn	Mục 6.2.3.4
1.4	**Bảo đảm an toàn dữ liệu**	**Mục 6.2.4**
1.4.1	Bảo mật dữ liệu	Mục 6.2.4.1
1.4.2	Sao lưu dự phòng	Mục 6.2.4.2

Phụ lục III
YÊU CẦU CƠ BẢN BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN ĐỐI VỚI HỆ THỐNG THÔNG TIN CẤP ĐỘ 3

(Ban hành kèm theo Quyết định số /QĐ-ĐHTN ngày ....tháng.....năm 2023 của Giám đốc Đại học Thái Nguyên)

I. YÊU CẦU QUẢN LÝ

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

1.5.6	Quản lý giám sát an toàn hệ thống thông tin	Mục 7.1.5.6
1.5.7	Quản lý điểm yếu an toàn thông tin	Mục 7.1.5.7
1.5.8	Quản lý sự cố an toàn thông tin	Mục 7.1.5.8
1.5.9	Quản lý an toàn người sử dụng đầu cuối	Mục 7.1.5.9
1.6	**Phương án Quản lý rủi ro an toàn thông tin**	
1.7	**Phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ**	

II. YÊU CẦU KỸ THUẬT

1. Yêu cầu về thiết kế hệ thống

a) Thiết kế các vùng mạng trong hệ thống theo chức năng, các vùng mạng tối thiểu bao gồm:

i. Vùng mạng nội bộ;

ii. Vùng mạng biên;

iii. Vùng DMZ;

iv. Vùng máy chủ nội bộ;

v. Vùng mạng không dây (nếu có) tách riêng, độc lập với các vùng mạng khác;

vi. Vùng mạng máy chủ cơ sở dữ liệu;

vii. Vùng quản trị.

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

i. Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn sử dụng mạng riêng ảo hoặc phương án tương đương; sử dụng sản phẩm Mạng riêng ảo đối với hệ thống thông tin có xử lý thông tin bí mật nhà nước hoặc hệ thống thông tin quy định tại điểm c khoản 2 Điều 9 Nghị định 85/2016/NĐ-CP ;

ii. Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập sử dụng sản phẩm Tường lửa có tích hợp chức năng phòng, chống xâm nhập hoặc sản phẩm Phòng, chống xâm nhập lớp mạng;

iii. Có phương án cân bằng tải, dự phòng nóng cho các thiết bị mạng chính, tối thiểu bao gồm thiết bị chuyển mạch trung tâm hoặc tương đương, thiết bị tường lửa trung tâm, tường lửa ứng dụng web, hệ thống lưu trữ tập trung, tường lửa cơ sở dữ liệu (nếu có);

iv. Có phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu; sử dụng sản phẩm Tường lửa cơ sở dữ liệu đối với hệ thống cơ sở dữ liệu tập trung, đáp ứng tiêu chí quy định tại khoản 3 Điều 9 Nghị định 85/2016/NĐ-CP ;

v. Có phương án chặn lọc phần mềm độc hại trên môi trường mạng sử dụng Tường lửa tích hợp chức năng phòng, chống mã độc trên môi trường mạng hoặc phương án tương đương;

vi. Có phương án phòng chống tấn công từ chối dịch vụ; sử dụng dịch vụ của doanh nghiệp hoặc sản phẩm Phòng, chống tấn công từ chối dịch vụ đối với các hệ thống Trung tâm dữ liệu, điện toán đám mây, hệ thống Định danh, xác thực điện tử, chứng thực điện tử, chữ ký số và hệ thống Kết nối tích hợp, chia sẻ dữ liệu, đáp ứng tiêu chí quy định tại khoản 3 Điều 9 Nghị định 85/2016/NĐ-CP ;

vii. Có phương án phòng chống tấn công mạng cho ứng dụng web; sử dụng sản phẩm Tường lửa ứng dụng web đối với các hệ thống thông tin được quy định tại khoản 2, Điều 9 Nghị định 85/2016/NĐ-CP ;

viii. Có phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử; sử dụng sản phẩm Bảo đảm an toàn thông tin cho hệ thống thư điện tử đối với hệ thống Thư điện tử, đáp ứng tiêu chí quy định tại khoản 2 Điều 9 Nghị định 85/2016/NĐ-CP ;

ix. Có phương án quản lý truy cập lớp mạng; sử dụng sản phẩm Quản lý truy cập lớp mạng đối với hệ thống Mạng nội bộ, Trung tâm giám sát điều hành an toàn thông tin mạng, đáp ứng tiêu chí quy định tại khoản 3 Điều 9 Nghị định 85/2016/NĐ-CP ;

x. Có phương án giám sát hệ thống thông tin tập trung;

xi. Có phương án giám sát an toàn hệ thống thông tin tập trung sử dụng sản phẩm Quản lý và phân tích sự kiện an toàn thông tin hoặc sản phẩm tương đương;

xii. Có phương án quản lý sao lưu dự phòng tập trung sử dụng hệ thống lưu trữ tập trung và sản phẩm quản lý lưu trữ tập trung;

xiii. Có phương án quản lý phần mềm phòng chống mã độc trên máy chủ/máy tính người dùng, sử dụng sản phẩm Phòng, chống mã độc và/hoặc sản phẩm Phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu cuối, có chức năng quản lý tập trung;

xiv. Có phương án phòng, chống thất thoát dữ liệu; sử dụng sản phẩm Phòng, chống thất thoát dữ liệu đối với hệ thống thông tin có xử lý thông tin bí mật nhà nước hoặc hệ thống thông tin quy định tại điểm c khoản 2 Điều 9 Nghị định 85/2016/NĐ-CP ;

xv. Có phương án dự phòng kết nối mạng Internet cho các máy chủ dịch vụ;

xvi. Có phương án bảo đảm an toàn cho mạng không dây (nếu có).

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

STT	Yêu cầu	TCVN 11930:2017
1.1	**Bảo đảm an toàn mạng**	**Mục 7.2.1**
1.1.1	Kiểm soát truy cập từ bên ngoài mạng	Mục 7.2.1.2
1.1.2	Kiểm soát truy cập từ bên trong mạng	Mục 7.2.1.3
1.1.3	Nhật kí hệ thống	Mục 7.2.1.4
1.1.4	Phòng chống xâm nhập	Mục 7.2.1.5

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

Phụ lục IV

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

(Ban hành kèm theo Quyết định số /QĐ-ĐHTN ngày ....tháng.....năm 2023 của Giám đốc Đại học Thái Nguyên)

Mẫu 01	Văn bản đề nghị thẩm định hồ sơ đề xuất cấp độ
Mẫu 02	Ý kiến thẩm định hồ sơ đề xuất cấp độ
Mẫu 03	Tờ trình phê duyệt hồ sơ đề xuất cấp độ
Mẫu 04	Quyết định phê duyệt cấp độ an toàn hệ thống thông tin
Mẫu 05	Quyết định phê duyệt phương án bảo đảm an toàn thông tin

Mẫu 01

TÊN ĐƠN VỊ -------	**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	*Thái Nguyên, ngày ... tháng ... năm ...*

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

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

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

(Tên cơ quan, tổ chức) đề nghị (Cơ quan thẩm định) thẩm định hồ sơ đề xuất cấp độ với các nội dung sau:

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 mô tả, thuyết minh tổng quan về hệ thống thông tin.
2. Tài liệu thiết kế thi công đã được cấp có thẩm quyền phê duyệt hoặc tài liệu có giá trị tương đương.
3. Tài liệu thuyết minh về việc đề xuất cấp độ căn cứ trên các tiêu chí theo quy định của pháp luật.
4. Tài liệu thuyết minh phương án bảo đảm an toàn thông tin theo cấp độ tương ứng.

(Tên cơ quan, tổ chức) đề nghị (Cơ quan thẩm định) cho ý kiến thẩm định hồ sơ đề xuất cấp độ an toàn hệ thống thông tin đối với (Tên hệ thống thông tin)./.

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

Mẫu 02

TÊN ĐƠN VỊ -------	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc** ----------
Số: ..... V/v ý kiến thẩm định hồ sơ đề xuất cấp độ	*Thái Nguyên, ngày ... tháng ... năm ...*

Kính gửi: (Chủ quản hệ thống thông tin/
Đơn vị vận hành hệ thống thông tin).

(Tên cơ quan thẩm định) nhận được Công văn số ..... ngày ..... tháng ..... năm ..... của (Tên cơ quan đề nghị) về việc thẩm định hồ sơ đề xuất cấp độ của hệ thống thông tin đối với (Tên hệ thống thông tin). Sau khi xem xét, tổng hợp ý kiến và kết quả thẩm định của các cơ quan, tổ chức có liên quan, (Tên cơ quan thẩm định) có ý kiến thẩm định như sau:

Phần 1. Hồ sơ, tài liệu thẩm định

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

2. Tài liệu thiết kế thi công đã được cấp có thẩm quyền phê duyệt hoặc tài liệu có giá trị tương đương.

3. Tài liệu thuyết minh về việc đề xuất cấp độ căn cứ trên các tiêu chí theo quy định của pháp luật.

4. Tài liệu thuyết minh phương án bảo đảm an toàn thông tin theo cấp độ tương ứng.

Phần 2. Căn cứ pháp lý để thẩm định

1. Căn cứ Luật an toàn thông tin mạng ngày 19 tháng 11 năm 2015.

2. Căn cứ các văn bản hướng dẫn thi hành Luật an toàn thông tin mạng.

2. Các căn cứ pháp lý khác có liên quan.

Phần 3. Tổ chức thẩm định

1. Đơn vị chủ trì thẩm định:

2. Đơn vị phối hợp thẩm định:

3. Hình thức thẩm định: Tổ chức họp hoặc lấy ý kiến bằng văn bản hoặc áp dụng cả hai hình thức (nếu cần thiết).

Phần 4. ý kiến thẩm định

1. Ý kiến thẩm định về sự phù hợp về việc đề xuất cấp độ theo quy định tại Điều 12 Quy định này.

2. Ý kiến khác (nếu có).

Phần 5. Kết luận

Hồ sơ đề xuất cấp độ hệ thống thông tin là phù hợp/chưa phù hợp (nếu chưa phù hợp đề nghị chỉ rõ những nội dung chưa phù hợp) để theo cấp độ đề xuất.

Trên đây là ý kiến thẩm định của (Cơ quan thẩm định) cho hồ sơ đề xuất cấp độ của hệ thống thông tin (Tên hệ thống thông tin). Đề nghị cơ quan (Tên cơ quan đề nghị) xem xét báo cáo cấp có thẩm quyền Điều chỉnh (nếu yêu cầu Điều chỉnh) hoặc trình cơ quan có thẩm quyền phê duyệt (nếu chấp thuận đề xuất của cơ quan trình)./.

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

Mẫu 03

TÊN ĐƠN VỊ -------	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc** ----------
Số: ……..	*Thái Nguyên, ngày ... tháng ... năm ...*

TỜ TRÌNH

Về việc phê duyệt đề xuất cấp độ

Kính gửi: (Cơ quan liên quan có thẩm quyền).

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

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

Căn cứ ý kiến thẩm định của đơn vị chuyên trách về công nghệ thông tin/cơ quan thẩm định;

(Tên cơ quan, tổ chức) trình phê duyệt hồ sơ đề xuất cấp độ với các nội dung sau:

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 mô tả, thuyết minh tổng quan về hệ thống thông tin.
2. Tài liệu thiết kế thi công đã được cấp có thẩm quyền phê duyệt hoặc tài liệu có giá trị tương đương.
3. Tài liệu thuyết minh về việc đề xuất cấp độ căn cứ trên các tiêu chí theo quy định của pháp luật.
4. Tài liệu thuyết minh phương án bảo đảm an toàn thông tin theo cấp độ tương ứng.
5. Ý kiến thẩm định của cơ quan chủ trì thẩm định đối với hệ thống thông tin đề xuất từ cấp độ 3 trở lên.

(Tên cơ quan) trình (Chủ quản hệ thống thông tin) xem xét, quyết định phê duyệt đề xuất cấp độ của hệ thống thông tin (Tên hệ thống thông tin)./.

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

Mẫu 04

CHỦ QUẢN HỆ THỐNG THÔNG TIN	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**
-------	**Độc lập - Tự do - Hạnh phúc**

Số: ……..	*Thái Nguyên, ngày ... tháng ... năm ...*

QUYẾT ĐỊNH

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

(THỦ TRƯỞNG CƠ QUAN TỔ CHỨC)

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

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

Xét đề nghị của cơ quan (Tên đơn vị đề nghị),

QUYẾT ĐỊNH:

Điều 1. Phê duyệt cấp độ an toàn hệ thống thông tin đối với (Tên hệ thống thông tin) cụ thể như sau:

1. Thông tin chung

a) Tên hệ thống thông tin:

b) Đơn vị vận hành hệ thống thông tin:

c) Địa chỉ:

2. Cấp độ an toàn hệ thống thông tin: (cấp độ)

3. Phương án bảo đảm an toàn thông tin:

a) Phương án bảo đảm an toàn thông tin trong thiết kế hệ thống thông tin tương ứng với cấp độ (cấp độ) là phù hợp với tiêu chuẩn quốc gia (Tên tiêu chuẩn), quy chuẩn kỹ thuật quốc gia (Tên quy chuẩn) về bảo đảm an toàn hệ thống thông tin theo cấp độ.

b) Phương án bảo đảm an toàn thông tin trong quá trình vận hành hệ thống tương ứng với cấp độ (cấp độ) là phù hợp với tiêu chuẩn quốc gia (Tên tiêu chuẩn), quy chuẩn kỹ thuật quốc gia (Tên quy chuẩn) về bảo đảm an toàn hệ thống thông tin theo cấp độ.

Điều 2. Tổ chức thực hiện

1. Cơ quan (Tên đơn vị đề nghị) chịu trách nhiệm:

a) Thực hiện trách nhiệm bảo đảm an toàn hệ thống thông tin mình quản lý theo các quy định tại Điều 23 Quy định này.

b) Các nội dung khác (nếu có).

2. Trách nhiệm của các cơ quan liên quan khác (nếu có).

Điều 3. Điều Khoản thi hành

1. Cơ quan (Tên đơn vị đề xuất) và các cơ quan liên quan khác chịu trách nhiệm thi hành Quyết định này.

2. Đơn vị chuyên trách về an toàn thông tin chịu trách nhiệm kiểm tra, giám sát việc thực hiện Quyết định này báo cáo cơ quan (Chủ quản hệ thống thông tin) theo quy định của pháp luật./.

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

Mẫu 05

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

QUYẾT ĐỊNH

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

THỦ TRƯỞNG CƠ QUAN TỔ CHỨC

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

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

Xét đề nghị của cơ quan (Tên đơn vị đề nghị),

QUYẾT ĐỊNH:

Điều 1. Phê duyệt phương án bảo đảm an toàn thông tin đối với (Tên hệ thống thông tin) cụ thể như sau:

1. Thông tin chung

a) Tên hệ thống thông tin:

b) Đơn vị vận hành hệ thống thông tin:

c) Địa chỉ:

2. Phương án bảo đảm an toàn thông tin:

a) Phương án bảo đảm an toàn thông tin trong thiết kế hệ thống thông tin tương ứng với cấp độ (cấp độ) là phù hợp với tiêu chuẩn quốc gia (Tên tiêu chuẩn), quy chuẩn kỹ thuật quốc gia (Tên quy chuẩn) về bảo đảm an toàn hệ thống thông tin theo cấp độ.

b) Phương án bảo đảm an toàn thông tin trong quá trình vận hành hệ thống tương ứng với cấp độ (cấp độ) là phù hợp với tiêu chuẩn quốc gia (Tên tiêu chuẩn), quy chuẩn kỹ thuật quốc gia (Tên quy chuẩn) về bảo đảm an toàn hệ thống thông tin theo cấp độ.

Điều 2. Tổ chức thực hiện

1. Cơ quan (Tên đơn vị đề nghị) chịu trách nhiệm:

a) Thực hiện trách nhiệm bảo đảm an toàn hệ thống thông tin mình quản lý theo các quy định tại Điều 22 Nghị định này.

b) Các nội dung khác (nếu có).

2. Trách nhiệm của các cơ quan liên quan khác (nếu có).

Điều 3. Điều Khoản thi hành

1. Cơ quan (Tên đơn vị đề xuất) và các cơ quan liên quan khác chịu trách nhiệm thi hành Quyết định này.

2. Đơn vị chuyên trách về an toàn thông tin chịu trách nhiệm kiểm tra, giám sát việc thực hiện Quyết định này báo cáo cơ quan (Chủ quản hệ thống thông tin) theo quy định của pháp luật./.

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