Cơ quan phát hành: VĂN PHÒNG CHÍNH PHỦ

CHÍNH PHỦ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 331/2026/NĐ-CP	*Hà Nội, ngày 19 tháng 8 năm 2026*

NGHỊ ĐỊNH
Về bảo vệ an ninh mạng đối với hệ thống thông tin

Căn cứ Luật Tổ chức Chính phủ số 63/2025/QH15;

Căn cứ Luật An ninh mạng số 116/2025/QH15;

Theo đề nghị của Bộ trưởng Bộ Công an;

Chính phủ ban hành Nghị định về bảo vệ an ninh mạng đối với hệ thống thông tin.

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Nghị định này quy định chi tiết khoản 2 Điều 8, khoản 5 Điều 9, khoản 6 Điều 10, khoản 5 Điều 12 Luật An ninh mạng, cụ thể: tiêu chí xác định cấp độ hệ thống thông tin; quy định thẩm quyền, trình tự, thủ tục xác định cấp độ hệ thống thông tin và biện pháp, trách nhiệm, nghĩa vụ bảo đảm an ninh mạng theo từng cấp độ của hệ thống thông tin; tiêu chí xác định hệ thống thông tin quan trọng về an ninh quốc gia; nhiệm vụ bảo vệ an ninh mạng đối với hệ thống thông tin; biện pháp bảo vệ an ninh mạng đối với hệ thống thông tin; kiểm tra an ninh mạng đối với hệ thống thông tin của cơ quan, tổ chức không thuộc danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

Điều 2. Đối tượng áp dụng

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

Khuyến khích tổ chức, cá nhân liên quan khác áp dụng các quy định tại Nghị định này để bảo vệ hệ thống thông tin.

LuatVietnam
Tiện ích văn bản luật

Điều 3. Giải thích từ ngữ

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

1. Xử lý thông tin là việc thực hiện một hoặc một số thao tác tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ, chia sẻ và trao đổi thông tin trên không gian mạng.

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

3. Bộ phận chuyên trách về an ninh mạng là bộ phận thuộc đơn vị chuyên trách về công nghệ thông tin hoặc chuyển đổi số, do chủ quản hệ thống thông tin thành lập hoặc chỉ định để thực thi nhiệm vụ bảo đảm an ninh mạng và ứng phó sự cố an ninh mạng (trường hợp không thành lập được đơn vị chuyên trách về an ninh mạng).

4. Cấp độ an ninh mạng hệ thống thông tin được hiểu là cấp độ hệ thống thông tin.

5. Dịch vụ trực tuyến là dịch vụ do doanh nghiệp hoặc cơ quan nhà nước cung cấp trên môi trường mạng cho các tổ chức, cá nhân.

Điều 4. Chủ quản hệ thống thông tin

1. Đối với các bộ, cơ quan ngang bộ, Ủy ban nhân dân cấp tỉnh, chủ quản hệ thống thông tin là:

a) Bộ, cơ quan ngang bộ;

b) Ủy ban nhân dân cấp tỉnh;

c) Cấp có thẩm quyền quyết định đầu tư dự án xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin. Bộ, cơ quan ngang bộ, Ủy ban nhân dân cấp tỉnh quyết định chủ quản hệ thống thông tin theo quy định của khoản này, bảo đảm cơ quan, tổ chức được giao chủ quản hệ thống thông tin có đủ năng lực để thực thi đầy đủ các quy định tại Điều 31 Nghị định này.

2. Đối với doanh nghiệp và tổ chức khác trừ quy định tại điểm a, điểm b khoản 1 Điều này, chủ quản hệ thống thông tin là cấp có thẩm quyền quyết định đầu tư xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin.

3. Trong trường hợp cần thiết, chủ quản hệ thống thông tin ủy quyền cho một tổ chức trực thuộc có đủ năng lực để thay mặt thực hiện trách nhiệm của chủ quản hệ thống thông tin quy định tại khoản 2 Điều 31 Nghị định này.

LuatVietnam
Tiện ích văn bản luật

Việc ủy quyền trách nhiệm chủ quản hệ thống thông tin phải được thực hiện bằng văn bản, trong đó nêu rõ phạm vi của hệ thống, trách nhiệm của tổ chức được ủy quyền và thời hạn ủy quyền.

Điều 5. 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.

2. Trong trường hợp hệ thống thông tin 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 có trách nhiệm chỉ định một đơn vị chủ trì 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 thuê dịch vụ công nghệ thông tin, đơn vị vận hành hệ thống thông tin được xác định như sau:

a) Trường hợp đã xác định được đơn vị cung cấp dịch vụ theo quy định của pháp luật, đơn vị vận hành được xác định theo thỏa thuận trong hợp đồng giữa các bên; hợp đồng phải quy định chi tiết trách nhiệm, thẩm quyền của các bên trong quản trị dữ liệu, kiểm soát truy cập, bảo đảm an ninh mạng, bảo đảm phù hợp với quy định của pháp luật dân sự và pháp luật về an ninh mạng;

b) Trường hợp hết thời hạn cung cấp dịch vụ, nếu hệ thống thông tin vẫn tiếp tục duy trì hoạt động, đơn vị vận hành được xác định theo các điều khoản cam kết duy trì, chuyển giao dịch vụ trong hợp đồng hoặc theo thỏa thuận mới giữa các bên;

c) Trường hợp khác, đơn vị chủ trì thuê dịch vụ đóng vai trò là đơn vị vận hành.

Điều 6. Nguyên tắc bảo đảm an ninh mạng hệ thống thông tin theo cấp độ

1. Việc bảo đảm an ninh mạng 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 ninh mạng 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 ninh mạng hệ thống thông tin thực hiện theo thứ tự ưu tiên từ cấp độ cao xuống cấp độ thấp.

LuatVietnam
Tiện ích văn bản luật

4. Bộ Quốc phòng quản lý về an ninh mạng với nhiệm vụ quân sự, quốc phòng; Bộ Công an quản lý về an ninh mạng đối với các hoạt động dân sự, kinh tế của các đơn vị quân đội theo thẩm quyền; các nội dung giao thoa (nếu có), Bộ Công an và Bộ Quốc phòng thống nhất bằng quy chế phối hợp.

Điều 7. Xác định hệ thống thông tin

1. Hệ thống thông tin phải có chức năng nghiệp vụ rõ ràng; có xử lý dữ liệu; có người dùng, đối tượng vận hành hoặc đối tượng phục vụ cụ thể; có kết quả đầu ra dưới dạng thông tin, dữ liệu phục vụ hoạt động quản lý, điều hành, giao dịch hoặc cung cấp dịch vụ.

2. Phạm vi của hệ thống thông tin:

a) Phạm vi của hệ thống thông tin phải được xác định trên cơ sở: chức năng nghiệp vụ (cùng phục vụ một chức năng hoặc quy trình nghiệp vụ cốt lõi); dòng chảy và mối liên kết dữ liệu (có trao đổi dữ liệu thường xuyên, liên tục hoặc phụ thuộc lẫn nhau trong xử lý); mức độ phụ thuộc trong vận hành (không thể vận hành độc lập mà không làm gián đoạn hoạt động của thành phần khác); phạm vi và mức độ ảnh hưởng khi xảy ra sự cố (sự cố của một thành phần có thể ảnh hưởng đến tính toàn vẹn hoặc làm gián đoạn chức năng, quy trình nghiệp vụ cốt lõi của toàn bộ hệ thống thông tin);

b) Việc xác định phạm vi hệ thống thông tin phải phản ánh đúng bản chất vận hành thực tế, không phụ thuộc vào cách tổ chức hành chính, mô hình triển khai kỹ thuật hoặc cấu trúc hạ tầng vật lý. Trường hợp các hệ thống có kết nối, liên thông dữ liệu hoặc chia sẻ tài nguyên hạ tầng, việc xác định phạm vi hệ thống phải xem xét khả năng lan truyền rủi ro và ảnh hưởng dây chuyền.

Điều 8. Nguyên tắc xác định cấp độ hệ thống thông tin

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, sản xuất, kinh doanh cụ thể của cơ quan, tổ chức thuộc một trong các loại hình hệ thống thông tin quy định tại khoản 2 Điều 9 Nghị định này.

2. Trường hợp hệ thống thông tin đồng thời đáp ứng nhiều tiêu chí thuộc các cấp độ khác nhau thì áp dụng cấp độ cao nhất.

3. Không xác định phạm vi hệ thống thông tin một cách hình thức nhằm làm thay đổi cấp độ hệ thống thông tin hoặc giảm yêu cầu bảo đảm an ninh mạng. Trường hợp phát hiện việc phân tách hoặc hợp nhất hệ thống thông tin không phù hợp với quy định, cơ quan, đơn vị có thẩm quyền yêu cầu xác định lại hệ thống thông tin và cấp độ tương ứng.

LuatVietnam
Tiện ích văn bản luật

Chương II
TIÊU CHÍ XÁC ĐỊNH CẤP ĐỘ HỆ THỐNG THÔNG TIN VÀ HỆ THỐNG THÔNG TIN QUAN TRỌNG VỀ AN NINH QUỐC GIA

Điều 9. Phân loại thông tin và hệ thống thông tin

1. Thông tin xử lý 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 cơ quan, tổ chức;

b) Hệ thống thông tin phục vụ người dân, doanh nghiệp là hệ thống trực tiếp hoặc hỗ trợ cung cấp dịch vụ trực tuyến, bao gồm dịch vụ công trực tuyến và dịch vụ trực tuyến khác trong các lĩnh vực viễn thông, công nghệ thông tin, thương mại, tài chính, ngân hàng, y tế, giáo dục và các lĩnh vực chuyên ngành khác;

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 cơ quan, tổ chức như mạng diện rộng, cơ sở dữ liệu, trung tâm dữ liệu, điện toán đám mây; xác thực điện tử, chứng thực điện tử, chữ ký số; kết nối liên thông các hệ thống thông tin;

d) Hệ thống thông tin điều khiển công nghiệp là hệ thống có chức năng giám sát, thu thập dữ liệu, quản lý và kiểm soát các hạng mục quan trọng phục vụ điều khiển, vận hành hoạt động bình thường của các công trình xây dựng;

LuatVietnam
Tiện ích văn bản luật

đ) Hệ thống thông tin khác là hệ thống thông tin không thuộc các loại hình được nêu tại các điểm a, b, c, d khoản này, được sử dụng để trực tiếp phục vụ hoặc hỗ trợ hoạt động nghiệp vụ, sản xuất, kinh doanh cụ thể của cơ quan, tổ chức theo lĩnh vực chuyên ngành;

e) Định kỳ hằng năm (trước ngày 15 tháng 01), Bộ Công an có trách nhiệm cập nhật, bổ sung danh mục các hệ thống thông tin theo quy định tại các điểm a, b, c, d, đ khoản này và công bố trên Cổng thông tin điện tử của Bộ Công an (trừ hệ thống thông tin quân sự và hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ).

Điều 10. Quản lý rủi ro an ninh mạng đối với hệ thống thông tin

1. Quản lý rủi ro an ninh mạng là quá trình xác định, đánh giá, xử lý và kiểm soát các rủi ro có thể gây tổn hại đến an ninh mạng của hệ thống thông tin, làm căn cứ hỗ trợ xác định cấp độ hệ thống thông tin và áp dụng biện pháp bảo đảm an ninh mạng phù hợp.

2. Chủ quản hệ thống thông tin có trách nhiệm thực hiện đánh giá rủi ro an ninh mạng trong các trường hợp sau đây:

a) Khi xác định cấp độ hệ thống thông tin lần đầu;

b) Khi có thay đổi về chức năng, phạm vi phục vụ, đối tượng sử dụng, loại thông tin xử lý hoặc công nghệ triển khai hệ thống thông tin;

c) Khi hệ thống thông tin mở rộng quy mô, tích hợp, kết nối liên thông hoặc chia sẻ dữ liệu với hệ thống khác;

d) Khi xảy ra sự cố an ninh mạng nghiêm trọng hoặc có nguy cơ cao ảnh hưởng đến an ninh quốc gia, trật tự, an toàn xã hội, lợi ích công cộng;

đ) Khi có yêu cầu của cơ quan nhà nước có thẩm quyền.

3. Nội dung đánh giá rủi ro an ninh mạng bao gồm tối thiểu các yếu tố sau đây:

a) Xác định tài sản, chức năng trọng yếu, vai trò của tài sản trong hệ thống thông tin và phân loại tài sản theo thứ tự quan trọng trong hệ thống thông tin;

b) Xác định loại thông tin được xử lý, lưu trữ, truyền đưa qua hệ thống, bao gồm thông tin công cộng, thông tin riêng, thông tin cá nhân, thông tin bí mật nhà nước;

c) Nhận diện rủi ro an ninh mạng dựa trên xác định mối đe dọa, điểm yếu, lỗ hổng bảo mật và khả năng bị khai thác;

LuatVietnam
Tiện ích văn bản luật

d) Đánh giá khả năng xảy ra sự cố và mức độ tác động, hậu quả đối với an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân, lợi ích công cộng;

đ) Đánh giá năng lực hiện có trong việc phòng ngừa, phát hiện, ứng phó và khắc phục sự cố an ninh mạng;

e) Xây dựng kế hoạch và triển khai các biện pháp giảm thiểu rủi ro tương ứng với các rủi ro đã xác định;

g) Thực hiện truyền thông rủi ro và báo cáo đến cơ quan có thẩm quyền.

4. Kết quả đánh giá rủi ro an ninh mạng là căn cứ để:

a) Đề xuất, xác định hoặc điều chỉnh cấp độ hệ thống thông tin theo quy định tại các Điều 11 đến Điều 16 Nghị định này;

b) Lựa chọn, triển khai biện pháp bảo đảm an ninh mạng tương ứng với cấp độ hệ thống thông tin;

c) Xây dựng, điều chỉnh phương án bảo vệ hệ thống thông tin, phương án ứng cứu sự cố an ninh mạng.

5. Trường hợp kết quả đánh giá rủi ro an ninh mạng cho thấy mức độ rủi ro cao hơn so với cấp độ đã được xác định, chủ quản hệ thống thông tin phải đề xuất áp dụng cấp độ cao hơn để bảo đảm an ninh mạng.

6. Chủ quản hệ thống thông tin có trách nhiệm lưu giữ hồ sơ đánh giá rủi ro an ninh mạng và cung cấp cho cơ quan nhà nước có thẩm quyền khi phục vụ công tác thanh tra, kiểm tra, giám sát theo quy định của pháp luật.

7. Cơ quan nhà nước có thẩm quyền, đơn vị chức năng căn cứ kết quả đánh giá rủi ro an ninh mạng để yêu cầu hay đề xuất chủ quản hệ thống thông tin rà soát, đánh giá lại cấp độ hệ thống thông tin và áp dụng biện pháp bảo đảm an ninh mạng phù hợp trong trường hợp cần thiết.

8. Việc đánh giá rủi ro an ninh mạng được thực hiện theo quy định của Bộ trưởng Bộ Công an (trừ hệ thống thông tin quân sự và hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ).

Điều 11. Tiêu chí xác định cấp độ 1

1. Hệ thống thông tin cấp độ 1 là hệ thống phục vụ hoạt động nội bộ của cơ quan, tổ chức và chỉ xử lý thông tin công cộng.

2. Hệ thống thông tin được đánh giá rủi ro an ninh mạng theo Khung quản lý rủi ro an ninh mạng.

LuatVietnam
Tiện ích văn bản luật

Điều 12. 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 sau:

1. Hệ thống thông tin phục vụ hoạt động nội bộ của cơ quan, tổ chức 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 vụ người dân, doanh nghiệp thuộc một trong các loại hình như sau:

a) Cung cấp dịch vụ trực tuyến không thuộc danh mục ngành, nghề đầu tư 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 100.000 chủ thể dữ liệu đối với dữ liệu cá nhân cơ bản hoặc dưới 10.000 chủ thể dữ liệu đối với dữ liệu cá nhân nhạy cảm.

3. Hệ thống cơ sở hạ tầng thông tin phục vụ hoạt động của một cơ quan, tổ chức.

4. Hệ thống thông tin khác do Thủ tướng Chính phủ quyết định hoặc được đánh giá rủi ro an ninh mạng theo Khung quản lý rủi ro an ninh mạng.

Điều 13. Tiêu chí xác định cấp độ 3

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

1. Hệ thống 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 an ninh quốc gia.

2. Hệ thống thông tin phục vụ người dân, doanh nghiệp thuộc một trong các loại hình như sau:

a) Cung cấp dịch vụ trực tuyến thuộc danh mục ngành, nghề đầu tư kinh doanh có điều kiện;

b) Hệ thống thông tin giải quyết thủ tục hành chính;

c) Cung cấp dịch vụ trực tuyến khác có xử lý thông tin riêng, thông tin cá nhân của từ 100.000 chủ thể dữ liệu đối với dữ liệu cá nhân cơ bản trở lên hoặc từ 10.000 chủ thể dữ liệu đối với dữ liệu cá nhân nhạy cảm trở lên.

3. Hệ thống cơ sở hạ tầng thông tin phục vụ hoạt động của các cơ quan, tổ chức trong phạm vi một bộ, một ngành, một tỉnh hoặc một số tỉnh.

LuatVietnam
Tiện ích văn bản luật

4. Hệ thống thông tin điều khiển công nghiệp trực tiếp phục vụ điều khiển, vận hành hoạt động bình thường của các công trình xây dựng cấp II, cấp III hoặc cấp IV theo phân cấp của pháp luật về xây dựng.

5. Hệ thống thông tin khác do Thủ tướng Chính phủ quyết định hoặc được đánh giá rủi ro an ninh mạng theo Khung quản lý rủi ro an ninh mạng.

Điều 14. Tiêu chí xác định cấp độ 4

Hệ thống thông tin cấp độ 4 là hệ thống có một trong các tiêu chí 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 nghiêm trọng tới an ninh quốc gia.

2. Hệ thống thông tin quốc gia phục vụ phát triển Chính phủ điện tử hoặc hệ thống cơ sở hạ tầng thông tin phục vụ hoạt động của các cơ quan, tổ chức trên phạm vi toàn quốc, yêu cầu vận hành 24/7 và không chấp nhận ngừng vận hành mà không có kế hoạch trước.

3. Hệ thống thông tin điều khiển công nghiệp trực tiếp phục vụ điều khiển, vận hành hoạt động bình thường của các công trình xây dựng cấp I theo phân cấp của pháp luật về xây dựng.

4. Hệ thống thông tin khác do Thủ tướng Chính phủ quyết định hoặc được đánh giá rủi ro an ninh mạng theo Khung quản lý rủi ro an ninh mạng.

Điều 15. Tiêu chí xác định cấp độ 5

Hệ thống thông tin cấp độ 5 là hệ thống có một trong các tiêu chí sau:

1. Hệ thống thông tin xử lý thông tin bí mật nhà nước hoặc hệ thống phục vụ quốc phòng, an ninh, mang tính chiến lược khi bị phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới an ninh quốc gia.

2. Hệ thống thông tin phục vụ lưu trữ dữ liệu tập trung đối với một số loại hình thông tin, dữ liệu đặc biệt quan trọng của quốc gia.

3. Hệ thống cơ sở hạ tầng thông tin quốc gia phục vụ kết nối liên thông hoạt động của Việt Nam với quốc tế.

4. Hệ thống thông tin điều khiển công nghiệp trực tiếp phục vụ điều khiển, vận hành hoạt động bình thường của công trình xây dựng cấp đặc biệt theo phân cấp của pháp luật về xây dựng hoặc công trình quan trọng liên quan đến an ninh quốc gia theo pháp luật về an ninh quốc gia.

LuatVietnam
Tiện ích văn bản luật

5. Hệ thống thông tin khác do Thủ tướng Chính phủ quyết định hoặc được đánh giá rủi ro an ninh mạng theo Khung quản lý rủi ro an ninh mạng.

Điều 16. Tiêu chí xác định hệ thống thông tin quan trọng về an ninh quốc gia

Hệ thống thông tin quan trọng về an ninh quốc gia đáp ứng một trong các tiêu chí sau đây:

1. Hệ thống thông tin phục vụ chỉ đạo, điều hành của các công trình quan trọng liên quan đến an ninh quốc gia theo quy định của pháp luật.

2. Hệ thống thông tin phục vụ chỉ đạo, điều hành, điều khiển hoạt động của công trình viễn thông quan trọng liên quan đến an ninh quốc gia theo quy định của pháp luật.

3. Hệ thống thông tin thuộc các lĩnh vực được quy định tại khoản 2 Điều 9 Luật An ninh mạng khi bị sự cố, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại sẽ gây ra một trong các hậu quả sau đây:

a) Trực tiếp tác động đến độc lập, chủ quyền, thống nhất và toàn vẹn lãnh thổ của Tổ quốc, sự tồn tại của chế độ và Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam;

b) Gây hậu quả nghiêm trọng đến an ninh quốc gia, đối ngoại làm suy yếu khả năng phòng thủ, bảo vệ Tổ quốc;

c) Gây hậu quả nghiêm trọng đến nền kinh tế quốc dân;

d) Gây thảm họa đối với đời sống con người, môi trường sinh thái;

đ) Gây hậu quả nghiêm trọng đến hoạt động của công trình xây dựng cấp đặc biệt theo phân cấp của pháp luật về xây dựng;

e) Gây hậu quả nghiêm trọng đến hoạt động hoạch định chủ trương, chính sách thuộc phạm vi bí mật nhà nước;

g) Ảnh hưởng nghiêm trọng đến sự chỉ đạo điều hành trực tiếp của các cơ quan Đảng, Nhà nước ở trung ương.

4. Hệ thống thông tin cấp độ 5 là hệ thống thông tin quan trọng về an ninh quốc gia.

LuatVietnam
Tiện ích văn bản luật

Điều 17. Lập hồ sơ đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia

1. Chủ quản hệ thống thông tin có trách nhiệm rà soát, đối chiếu với quy định tại Điều 16 Nghị định này, lập hồ sơ đề nghị đưa hệ thống thông tin thuộc thẩm quyền quản lý của mình vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

2. Trường hợp hệ thống thông tin trong quá trình thẩm định về cấp độ hệ thống thông tin mà xét thấy có đủ căn cứ để đưa vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia, chủ quản hệ thống thông tin lập hồ sơ đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

3. Lực lượng chuyên trách bảo vệ an ninh mạng căn cứ chức năng, nhiệm vụ được giao rà soát các hệ thống thông tin có căn cứ phù hợp với quy định tại Điều 16 Nghị định này và yêu cầu chủ quản hệ thống thông tin lập hồ sơ đề nghị đưa hệ thống thông tin thuộc thẩm quyền quản lý của mình vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

4. Hồ sơ đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia theo quy định tại Điều 21 Nghị định này.

Chương III
THẨM QUYỀN, TRÌNH TỰ, THỦ TỤC XÁC ĐỊNH CẤP ĐỘ, ĐỐI VỚI HỆ THỐNG THÔNG TIN

Điều 18. 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:

Đơn vị chuyên trách về an ninh mạng 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, gửi báo cáo chủ quản hệ thống thông tin.

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

a) Đơn vị chuyên trách về an ninh mạng của chủ quản hệ thống thông tin thực hiện thẩm định hồ sơ đề xuất cấp độ;

b) Chủ quản hệ thống thông tin phê duyệt hồ sơ đề xuất cấp độ.

3. Đối với hệ thống thông tin được đề xuất là cấp độ 4 hoặc cấp độ 5:

a) Bộ Công an chủ trì, phối hợp với chủ quản hệ thống thông tin và các bộ, ngành có liên quan thực hiện thẩm định hồ sơ đề xuất cấp độ hệ thống thông tin, trừ trường hợp quy định tại điểm b, điểm c khoản 3 Điều này. Bộ Công an

LuatVietnam
Tiện ích văn bản luật

chủ trì thực hiện thẩm định hồ sơ đề xuất cấp độ đối với hệ thống thông tin của cơ quan, tổ chức thuộc phạm vi quản lý của Bộ Công an;

b) Bộ Quốc phòng chủ trì thực hiện thẩm định hồ sơ đề xuất cấp độ đối với hệ thống thông tin quân sự;

c) Ban Cơ yếu Chính phủ chủ trì thực hiện thẩm định hồ sơ đề xuất cấp độ đối với hệ thống thông tin cơ yếu của cơ quan, tổ chức thuộc Ban Cơ yếu Chính phủ;

d) Chủ quản hệ thống thông tin phê duyệt hồ sơ đề xuất cấp độ đối với hệ thống thông tin cấp độ 4; phê duyệt phương án bảo đảm an ninh mạng đối với hệ thống thông tin cấp độ 5;

đ) Thủ tướng Chính phủ phê duyệt Danh mục hệ thống thông tin cấp độ 5 (Danh mục Hệ thống thông tin quan trọng về an ninh quốc gia).

4. Trường hợp đơn vị chuyên trách về an ninh mạng 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 ninh mạng 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 ninh mạng 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.

Điều 19. Trường hợp 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 dựollollng 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 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 tại Nghị định này.

2. Trong trường hợp thuê dịch vụ công nghệ thông tin:

a) 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 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 Nghị định này;

LuatVietnam
Tiện ích văn bản luật

b) Đơn vị cung cấp dịch vụ có trách nhiệm phối hợp với chủ quản hệ thống thông tin, đơn vị chủ trì thuê dịch vụ cập nhật thông tin trong hồ sơ đề xuất cấp độ theo hiện trạng hạ tầng đã cài đặt để tổ chức thẩm định, phê duyệt.

3. Tài liệu thuyết minh đề xuất cấp độ theo quy định tại Điều 21 Nghị định này.

Điều 20. 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 21 Nghị 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 18 Nghị 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 18 Nghị định này;

d) Đối với hệ thống thông tin được đề xuất là cấp độ 4 hoặc cấp độ 5:

Đơn vị vận hành hệ thống thông tin gửi hồ sơ đề xuất cấp độ tới đơn vị chuyên trách về an ninh mạng của chủ quản hệ thống thông tin để xin ý kiến chuyên môn về sự phù hợp của đề xuất cấp độ và phương án bảo đảm an ninh mạng hệ thống thông tin theo cấp độ;

Đơn vị vận hành hệ thống thông tin trình chủ quản hệ thống thông tin hồ sơ đề xuất cấp độ gửi tới cơ quan thẩm định quy định tại điểm a, điểm b hoặc điểm c khoản 3 Điều 18 Nghị định này.

2. Thẩm định hồ sơ đề xuất cấp độ:

Cơ quan có thẩm quyền thực hiện thẩm định hồ sơ đề xuất cấp độ theo quy định tại Điều 23 Nghị 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 ninh mạng của chủ quản hệ thống thông tin phê duyệt đề xuất cấp độ, gửi báo cáo chủ quản hệ thống thông tin;

LuatVietnam
Tiện ích văn bản luật

b) Đối với hệ thống thông tin được đề xuất là cấp độ 3 hoặc cấp độ 4: đơn vị vận hành hệ thống thông tin trình chủ quản hệ thống thông tin phê duyệt đề xuất cấp độ;

c) Đối với hệ thống thông tin được đề xuất là cấp độ 5:

Trên cơ sở kết quả thẩm định hồ sơ đề xuất cấp độ, Bộ Công an chủ trì, phối hợp với các bộ, ngành, cơ quan, tổ chức, cá nhân có liên quan trình Thủ tướng Chính phủ phê duyệt Danh mục hệ thống thông tin quan trọng về an ninh quốc gia;

Đơn vị vận hành hệ thống thông tin trình chủ quản hệ thống thông tin phê duyệt phương án bảo đảm an ninh mạng.

4. Đối với hệ thống thông tin cấp độ 3, cấp độ 4 được xác định thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia. Các đơn vị thực hiện trình tự, thủ tục xác định cấp độ đối với hệ thống thông tin như đối với hệ thống thông tin được đề xuất cấp độ 5.

Điều 21. 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 căn cứ trên các tiêu chí theo quy định của pháp luật.

4. Tài liệu thuyết minh phương án bảo đảm an ninh mạng theo cấp độ tương ứng.

5. Ý kiến về mặt chuyên môn của đơn vị chuyên trách về an ninh mạng đối với hệ thống thông tin đề xuất cấp độ 4 hoặc cấp độ 5.

Điều 22. Thuyết minh Hồ sơ đề xuất cấp độ 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

LuatVietnam
Tiện ích văn bản luật

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 ninh mạng 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 ninh mạng.

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;

LuatVietnam
Tiện ích văn bản luật

c) Nhận diện sơ bộ các nguy cơ, rủi ro an ninh mạng chính có thể phát sinh đối với hệ thống thông tin và mức độ ảnh hưởng dự kiến, làm căn cứ hỗ trợ đề xuất cấp độ.

5. Đối với hệ thống thông tin được đề xuất cấp độ 4 hoặc cấp độ 5, việc thuyết minh đề xuất cấp độ phải bao gồm báo cáo đánh giá rủi ro an ninh mạng ở mức độ chi tiết hơn, ngoài các nội dung được quy định tại khoản 3 Điều này, cần làm rõ thêm các nội dung sau đây:

a) Xác định các hệ thống thông tin khác có liên quan hoặc có kết nối đến hoặc có ảnh hưởng quan trọng tới hoạt động bình thường của hệ thống thông tin được đề xuất cấp độ;

b) Thuyết minh về các nguy cơ tấn công mạng và mức độ ảnh hưởng đối với hệ thống thông tin được đề xuất cấp độ;

c) Đánh giá phạm vi và mức độ ảnh hưởng tới lợi ích công cộng, trật tự, an toàn xã hội hoặc an ninh quốc gia khi bị tấn công mạng gây mất an ninh mạng hoặc gián đoạn hoạt động của hệ thống thông tin được đề xuất cấp độ;

d) Thuyết minh yêu cầu cần phải vận hành 24/7 và không chấp nhận ngừng vận hành mà không có kế hoạch trước đối với các hệ thống thông tin theo quy định tại khoản 2 Điều 14 Nghị định này.

6. Thuyết minh phương án bảo đảm an ninh mạng đáp ứng các yêu cầu về quản lý, kỹ thuật tương ứng với cấp độ đề xuất; trong đó mô tả chi tiết về phương án triển khai đối với từng yêu cầu.

Điều 23. 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 ninh mạng 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 ninh mạng hệ thống thông tin trong quá trình vận hành hệ thống theo cấp độ tương ứng.

2. Thời gian phản hồi đối với các hồ sơ chưa hợp lệ

Đối với hệ thống thông tin đề xuất cấp độ, thời gian phản hồi, hướng dẫn bổ sung tối đa là 05 ngày làm việc kể từ ngày nhận hồ sơ.

LuatVietnam
Tiện ích văn bản luật

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

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

b) Đối với hệ thống thông tin đề xuất cấp độ 4 hoặc cấp độ 5, thời gian thẩm định tối đa là 25 ngày làm việc kể từ ngày nhận đủ hồ sơ hợp lệ.

Điều 24. 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 25. 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
KIỂM TRA AN NINH MẠNG ĐỐI VỚI HỆ THỐNG THÔNG TIN CỦA CƠ QUAN, TỔ CHỨC KHÔNG THUỘC DANH MỤC HỆ THỐNG THÔNG TIN QUAN TRỌNG VỀ AN NINH QUỐC GIA

Điều 26. Trình tự, thủ tục kiểm tra an ninh mạng

1. Trình tự, thủ tục kiểm tra an ninh mạng của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an theo quy định tại khoản 4 Điều 12 Luật An ninh mạng:

a) Thông báo về kế hoạch kiểm tra an ninh mạng theo quy định;

b) Thành lập Đoàn kiểm tra theo chức năng, nhiệm vụ được giao;

c) Tiến hành kiểm tra an ninh mạng, phối hợp chặt chẽ với chủ quản hệ thống thông tin trong quá trình kiểm tra;

d) Lập biên bản về quá trình, kết quả kiểm tra an ninh mạng và bảo quản theo quy định của pháp luật;

LuatVietnam
Tiện ích văn bản luật

đ) Thông báo kết quả kiểm tra an ninh mạng sau khi hoàn thành kiểm tra.

2. Trường hợp cần giữ nguyên hiện trạng hệ thống thông tin, phục vụ điều tra, xử lý hành vi vi phạm pháp luật; hướng dẫn hoặc tham gia khắc phục khi có đề nghị của chủ quản hệ thống thông tin, lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an gửi văn bản đề nghị chủ quản hệ thống thông tin tạm ngừng tiến hành kiểm tra an ninh mạng. Nội dung văn bản phải ghi rõ lý do, mục đích, thời gian tạm ngừng hoạt động kiểm tra an ninh mạng. Bên cạnh đó, chủ quản hệ thống thông tin phải thiết lập phương án dự phòng, bảo đảm tính liên tục của hệ thống trước khi thực hiện cách ly hiện trạng, trừ trường hợp khẩn cấp để ngăn chặn ngay hành vi xâm phạm an ninh quốc gia.

3. Việc kiểm tra đối với hệ thống thông tin quân sự thuộc phạm vi quản lý của Bộ Quốc phòng do Bộ Quốc phòng chủ trì thực hiện hoặc có sự thống nhất bằng văn bản của Bộ Quốc phòng.

4. Việc kiểm tra đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ do Ban Cơ yếu Chính phủ chủ trì thực hiện hoặc có sự thống nhất bằng văn bản của Ban Cơ yếu Chính phủ.

Điều 27. Quy định về hoạt động kiểm tra, đánh giá an ninh mạng

1. Nội dung kiểm tra, đánh giá việc tuân thủ quy định của pháp luật về bảo đảm an ninh mạng 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 31 Nghị định này, bao gồm: việc thực hiện thành lập/chỉ định đơn vị chuyên trách/bộ phận chuyên trách về an ninh mạng của chủ quản hệ thống thông tin theo quy định tại khoản 1 Điều 31 Nghị định này; 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 ninh mạng 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 ninh mạng và quản lý rủi ro an ninh mạng trong phạm vi cơ quan, tổ chức của mình theo quy định tại điểm c khoản 2 Điều 31 Nghị định này; việc tổ chức thực hiện đào tạo ngắn hạn, tuyên truyền, phổ biến, nâng cao nhận thức và diễn tập về an ninh mạng theo quy định tại khoản 3 Điều 31 Nghị định này;

b) Kiểm tra, đánh giá tuân thủ đối với đơn vị chuyên trách về an ninh mạng của chủ quản hệ thống thông tin theo quy định tại Điều 32 Nghị định này, bao gồm các nội dung: công tác tham mưu, tổ chức thực thi, đôn đốc, kiểm tra, giám sát công tác bảo đảm an ninh mạng; 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;

LuatVietnam
Tiện ích văn bản luật

c) Kiểm tra, đánh giá tuân thủ đối với đơn vị vận hành theo quy định khoản 1 Điều 33 Nghị định này;

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

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

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

b) Đánh giá việc tuân thủ các quy định, quy trình trong Quy chế bảo đảm an ninh mạng 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 ninh mạng được phê duyệt;

d) Đánh giá việc thiết lập, cấu hình hệ thống theo phương án bảo đảm an ninh mạng 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.

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) Việc duy trì, cập nhật và khắc phục các tồn tại, điểm yếu, lỗ hổng bảo mật đã được phát hiện trong quá trình vận hành hệ thống;

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

d) 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.

4. 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).

LuatVietnam
Tiện ích văn bản luật

Chương V
NHIỆM VỤ, BIỆN PHÁP, TRÁCH NHIỆM BẢO ĐẢM AN NINH MẠNG ĐỐI VỚI HỆ THỐNG THÔNG TIN

Điều 28. Biện pháp bảo vệ an ninh mạng đối với hệ thống thông tin

1. Ban hành quy định về bảo đảm an ninh mạng trong thiết kế, xây dựng, quản lý, vận hành, sử dụng, nâng cấp, hủy bỏ hệ thống thông tin; tổ chức triển khai các biện pháp lưu trữ, sao lưu bảo vệ an ninh thông tin mạng và an ninh của các thành tố cấu thành hệ thống thông tin theo Tiêu chuẩn quốc gia về An ninh mạng - Hệ thống thông tin - Yêu cầu cơ bản.

2. Xác định, lập hồ sơ đề xuất cấp độ hệ thống thông tin, hệ thống thông tin quan trọng về an ninh quốc gia; tổ chức thẩm định an ninh mạng đối với hồ sơ, thiết kế hệ thống thông tin theo trình tự, thủ tục thẩm định hồ sơ đề xuất cấp độ được quy định chi tiết trong Chương III của Nghị định này.

3. Đánh giá điều kiện an ninh mạng hệ thống thông tin là hoạt động xem xét mức độ đáp ứng các điều kiện về an ninh mạng của hệ thống thông tin trước khi đưa vào vận hành, sử dụng.

a) Nội dung đánh giá điều kiện an ninh mạng bao gồm: chính sách, quy chế, quy trình bảo đảm an ninh mạng; tổ chức bộ máy, nhân sự phụ trách an ninh mạng; biện pháp quản lý và kỹ thuật bảo vệ an ninh mạng hệ thống thông tin; khả năng giám sát, phát hiện, ứng phó và khắc phục sự cố an ninh mạng; việc tuân thủ quy định của pháp luật về an ninh mạng và các quy định có liên quan;

b) Đánh giá điều kiện an ninh mạng được thực hiện trong trường hợp: trước khi đưa hệ thống thông tin vào vận hành; khi có thay đổi lớn về chức năng, quy mô, công nghệ hoặc mức độ rủi ro an ninh mạng; theo yêu cầu của cơ quan có thẩm quyền;

c) Kết quả đánh giá điều kiện an ninh mạng là căn cứ để: xác định hệ thống thông tin đủ hoặc không đủ điều kiện đưa vào vận hành, sử dụng; yêu cầu bổ sung, hoàn thiện các biện pháp bảo đảm an ninh mạng; phục vụ công tác quản lý nhà nước về an ninh mạng.

4. Áp dụng biện pháp quản lý, biện pháp kỹ thuật theo quy định tại Điều 29, Điều 30 Nghị định này, Tiêu chuẩn quốc gia về An ninh mạng - Hệ thống thông tin - Yêu cầu cơ bản và các tiêu chuẩn, quy chuẩn kỹ thuật về an ninh mạng khác theo quy định của pháp luật.

LuatVietnam
Tiện ích văn bản luật

5. Việc kiểm tra, giám sát việc tuân thủ quy định và đánh giá hiệu quả của các biện pháp quản lý, kỹ thuật được thực hiện theo hướng dẫn tại Điều 27 Nghị định này.

a) Hoạt động kiểm tra, giám sát và đánh giá hiệu quả được thực hiện: định kỳ theo cấp độ hệ thống thông tin và mức độ rủi ro an ninh mạng; thường xuyên thông qua hoạt động giám sát an ninh mạng; đột xuất khi có dấu hiệu vi phạm quy định về bảo đảm an ninh mạng hoặc nguy cơ mất an ninh mạng; theo yêu cầu của cơ quan có thẩm quyền;

b) Việc đánh giá hiệu quả các biện pháp bảo đảm an ninh mạng phải bảo đảm: xác định được mức độ hiệu quả của các biện pháp trong việc giảm thiểu rủi ro an ninh mạng; đánh giá khả năng đáp ứng yêu cầu bảo vệ hệ thống thông tin theo cấp độ; làm căn cứ để điều chỉnh, bổ sung hoặc thay thế các biện pháp quản lý và kỹ thuật không còn phù hợp;

c) Kết quả kiểm tra, giám sát và đánh giá hiệu quả là căn cứ: để tổ chức khắc phục, xử lý các tồn tại, điểm yếu, lỗ hổng bảo mật; phục vụ công tác quản lý nhà nước về an ninh mạng.

6. Bộ trưởng Bộ Công an quy định về hoạt động giám sát an ninh mạng, ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin.

Điều 29. Phương án bảo đảm an ninh mạng

1. Phương án bảo đảm an ninh mạng đối với hệ thống thông tin theo cấp độ, phương án bảo đảm an ninh mạng hệ thống thông tin quan trọng về an ninh quốc gia phải đáp ứng yêu cầu cơ bản quy định tại Nghị định này, Tiêu chuẩn quốc gia về An ninh mạng - Hệ thống thông tin - Yêu cầu cơ bản.

2. Phương án bảo đảm an ninh mạng bao gồm các nội dung sau đây:

a) Bảo đảm an ninh mạng trong thiết kế, xây dựng;

b) Bảo đảm an ninh mạng hệ thống thông tin trong quá trình vận hành;

c) Kiểm tra, đánh giá an ninh mạng;

d) Quản lý rủi ro an ninh mạng;

đ) Giám sát an ninh mạng;

e) Dự phòng, ứng phó sự cố an ninh mạng, khôi phục sau thảm họa;

g) Kết thúc vận hành, khai thác, thanh lý, hủy bỏ.

LuatVietnam
Tiện ích văn bản luật

Điều 30. Yêu cầu chung về bảo đảm an ninh mạng theo cấp độ

1. Việc bảo đảm an ninh mạng hệ thống thông tin theo cấp độ thực hiện theo yêu cầu cơ bản quy định tại Nghị định này và Tiêu chuẩn quốc gia về An ninh mạng - Hệ thống thông tin - Yêu cầu cơ bản.

2. Yêu cầu cơ bản về bảo đảm an ninh mạng đối với từng cấp độ hệ thống thông tin theo quy định tại Nghị định này là các yêu cầu tối thiểu để bảo đảm an ninh mạng, bao gồm yêu cầu cơ bản về quản lý, yêu cầu cơ bản về kỹ thuật và không bao gồm các yêu cầu bảo đảm an ninh vật lý.

3. Yêu cầu cơ bản về quản lý, bao gồm việc ban hành các quy định và triển khai các quy định về quản lý:

a) Thiết lập chính sách an ninh mạng;

b) Tổ chức bảo đảm an ninh mạng;

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 ninh mạng;

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 ninh mạng đáp ứng yêu cầu kỹ thuật cơ bản theo từng cấp độ thực hiện theo nguyên tắc quy định tại khoản 2 Điều 6 Nghị định này, cụ thể như sau:

a) Đối với hệ thống thông tin cấp độ 1, 2, 3: phương án bảo đảm an ninh mạng 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;

LuatVietnam
Tiện ích văn bản luật