VĂN BẢN QUY PHẠM PHÁP LUẬT

CHÍNH PHỦ

CHÍNH PHỦ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 53/2022/NĐ-CP	*Hà Nội, ngày 15 tháng 8 năm 2022*

NGHỊ ĐỊNH
Quy định chi tiết một số điều của Luật An ninh mạng

Căn cứ Luật Tổ chức Chính phủ ngày 19 tháng 6 năm 2015; Luật sửa đổi, bổ sung một số điều của Luật Tổ chức Chính phủ và Luật Tổ chức chính quyền địa phương ngày 22 tháng 11 năm 2019;

Căn cứ Luật An ninh quốc gia ngày 03 tháng 12 năm 2004;

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

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

Theo đề nghị của Bộ trưởng Bộ Công an;

Chính phủ ban hành Nghị định quy định chi tiết một số điều của Luật An ninh mạng.

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Nghị định này quy định chi tiết điểm a, b, c, d, đ, g, i, k, l khoản 1 Điều 5, khoản 4 Điều 10, khoản 5 Điều 12, khoản 1 Điều 23, khoản 7 Điều 24, khoản 2, 4 Điều 26, khoản 5 Điều 36 Luật An ninh mạng, gồm các nội dung sau:

1. Các biện pháp bảo vệ an ninh mạng: thẩm định an ninh mạng; đánh giá điều kiện an ninh mạng; kiểm tra an ninh mạng; giám sát an ninh mạng; ứng phó, khắc phục sự cố an ninh mạng; sử dụng mật mã để bảo vệ thông tin mạng; yêu cầu xóa bỏ thông tin trái pháp luật hoặc thông tin sai sự thật trên không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; thu thập dữ liệu điện tử liên quan đến hoạt động xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ

chức, cá nhân trên không gian mạng; đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin, thu hồi tên miền.

2. Căn cứ, trình tự, thủ tục xác lập và công tác phối hợp giữa các bộ, ngành chức năng có liên quan trong thẩm định, đánh giá, kiểm tra, giám sát, ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia.

3. Điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia.

4. Nội dung triển khai hoạt động bảo vệ an ninh mạng trong cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương.

5. Trình tự, thủ tục kiểm tra an ninh mạng đối với hệ thống thông tin của cơ quan, tổ chức, cá nhân không thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia theo các trường hợp được quy định tại khoản 1 Điều 24.

6. Việc lưu trữ dữ liệu và đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam đối với các doanh nghiệp được quy định tại khoản 3 Điều 26.

7. Việc phân công, phối hợp thực hiện các biện pháp bảo vệ an ninh mạng, phòng ngừa, xử lý hành vi xâm phạm an ninh mạng trong trường hợp nội dung quản lý nhà nước liên quan đến phạm vi quản lý của nhiều bộ, ngành.

Điều 2. Giải thích từ ngữ

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

1. Dữ liệu về thông tin cá nhân là dữ liệu về thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự để xác định danh tính một cá nhân.

2. Người sử dụng dịch vụ là tổ chức, cá nhân tham gia sử dụng dịch vụ trên không gian mạng.

3. Người sử dụng dịch vụ tại Việt Nam là tổ chức, cá nhân sử dụng không gian mạng trên lãnh thổ nước Cộng hòa xã hội chủ nghĩa Việt Nam.

4. Dữ liệu về mối quan hệ của người sử dụng dịch vụ là dữ liệu về thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự phản ánh, xác định mối quan hệ của người sử dụng dịch vụ với người khác trên không gian mạng.

5. Dữ liệu do người sử dụng dịch vụ tại Việt Nam tạo ra là dữ liệu về thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự phản ánh quá trình tham gia, hoạt động, sử dụng không gian mạng của người sử dụng dịch vụ và các thông tin về thiết bị, dịch vụ mạng sử dụng để kết nối với không gian mạng trên lãnh thổ nước Cộng hòa xã hội chủ nghĩa Việt Nam.

6. Dịch vụ trên mạng viễn thông là dịch vụ viễn thông, dịch vụ ứng dụng viễn thông theo quy định của pháp luật.

7. Dịch vụ trên mạng Internet là dịch vụ Internet và dịch vụ cung cấp nội dung trên nền internet theo quy định của pháp luật.

8. Dịch vụ gia tăng trên không gian mạng là dịch vụ viễn thông giá trị gia tăng theo quy định của pháp luật.

9. Lực lượng chuyên trách bảo vệ an ninh mạng bao gồm:

a) Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an;

b) Cục Bảo vệ an ninh Quân đội, Tổng cục Chính trị và Bộ Tư lệnh Tác chiến không gian mạng thuộc Bộ Quốc phòng.

10. Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia là cơ quan, tổ chức có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin quan trọng về an ninh quốc gia, gồm những trường hợp sau:

a) Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;

b) Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương;

c) Các tổ chức chính trị ở Trung ương;

d) Cấp có thẩm quyền quyết định đầu tư dự án xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin quan trọng về an ninh quốc gia.

11. Doanh nghiệp trong nước là doanh nghiệp được thành lập hoặc đăng ký thành lập theo pháp luật Việt Nam và có trụ sở chính tại Việt Nam.

12. Doanh nghiệp nước ngoài là doanh nghiệp được thành lập hoặc đăng ký thành lập theo pháp luật nước ngoài.

Chương II
XÁC LẬP DANH MỤC, CƠ CHẾ PHỐI HỢP, ĐIỀU KIỆN AN NINH MẠNG BẢO VỆ HỆ THỐNG THÔNG TIN QUAN TRỌNG VỀ AN NINH QUỐC GIA

Mục 1
XÁC LẬP DANH MỤC HỆ THỐNG THÔNG TIN QUAN TRỌNG VỀ AN NINH QUỐC GIA

Điều 3. Căn cứ xác lập hệ thống thông tin quan trọng về an ninh quốc gia

Hệ thống thông tin quan trọng về an ninh quốc gia là hệ thống thông tin của cơ quan nhà nước và tổ chức chính trị của nước Cộng hòa xã hội chủ nghĩa Việt Nam, bao gồm:

1. Hệ thống thông tin quan trọng quốc gia theo quy định của Luật An toàn thông tin mạng.

2. 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.

3. 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.

4. Hệ thống thông tin thuộc các lĩnh vực được quy định tại khoản 2 Điều 10 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 quốc phòng, 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.

Điều 4. 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 khoản 4 Điều 3 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. Đối với hệ thống thông tin thuộc Danh mục hệ thống thông tin quan trọng quốc gia:

a) Bộ Thông tin và Truyền thông có trách nhiệm gửi Bộ Công an hồ sơ hệ thống thông tin quan trọng quốc gia đã được Thủ tướng Chính phủ phê duyệt để xác lập Danh mục hệ thống thông tin quan trọng về an ninh quốc gia;

b) Trong trường hợp quy định tại điểm a khoản 2 Điều này, chủ quản hệ thống thông tin quan trọng quốc gia không phải lập hồ sơ đề nghị đưa hệ thống vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia;

c) Bộ Công an có trách nhiệm đưa những hệ thống thông tin quan trọng quốc gia vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia theo trình tự, thủ tục quy định; thông báo cho chủ quản các hệ thống thông tin này về việc hệ thống thông tin được đưa vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia và thực hiện các trách nhiệm tương ứng.

3. Trường hợp hệ thống thông tin trong quá trình thẩm định về cấp độ an toàn 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, Bộ Thông tin và Truyền thông có trách nhiệm chuyển hồ sơ cho Bộ Công an để thẩm định hồ sơ đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

4. 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 3 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.

5. Hồ sơ đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia:

a) Văn bản đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia (Mẫu số 01 Phụ lục);

b) Văn bản cung cấp danh mục toàn bộ hệ thống thông tin của cơ quan, tổ chức (Mẫu số 02 Phụ lục);

c) Tài liệu chứng minh kèm theo, gồm: Tài liệu mô tả, thuyết minh tổng quan về hệ thống thông tin; tài liệu thiết kế thi công đã được cấp có thẩm quyền phê duyệt hoặc tài liệu có giá trị tương đương; tài liệu chứng minh sự phù hợp với căn cứ đề xuất đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về

an ninh quốc gia; tài liệu thuyết minh phương án bảo vệ hệ thống thông tin (phương án bảo đảm an toàn hạ tầng mạng; an toàn máy chủ; an toàn ứng dụng; an toàn cơ sở dữ liệu; chính sách quản lý; tổ chức, nhân sự; quản lý thiết kế, xây dựng; quản lý vận hành; kiểm tra, đánh giá và quản lý rủi ro).

6. Hồ sơ đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia được lập thành 01 bản chính, gửi về:

a) Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an, trừ quy định tại điểm b và điểm c khoản này;

b) Bộ Tư lệnh Tác chiến không gian mạng thuộc Bộ Quốc phòng đối với các hệ thống thông tin quân sự.

c) Ban Cơ yếu Chính phủ đối với các hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ.

7. Cơ quan tiếp nhận hồ sơ tại khoản 6 Điều này có trách nhiệm phản hồi ý kiến bằng văn bản về hồ sơ đã tiếp nhận (Mẫu số 03 Phụ lục).

Điều 5. Thẩm định hồ sơ đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia

1. Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an thẩm định 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, trừ trường hợp quy định tại khoản 2 và khoản 3 Điều này.

2. Bộ Tư lệnh Tác chiến không gian mạng thuộc Bộ Quốc phòng hướng dẫn lập hồ sơ, tiếp nhận và thẩm định hồ sơ đề nghị đưa hệ thống thông tin quân sự vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

3. Ban Cơ yếu Chính phủ thẩm định hồ sơ đề nghị đưa hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

4. Hội đồng thẩm định hồ sơ đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia:

a) Đối với hệ thống thông tin quan trọng về an ninh quốc gia có liên quan tới nhiều ngành, lĩnh vực hoặc việc thẩm định cần có ý kiến của nhiều bộ, ngành chức năng;

b) Hội đồng thẩm định làm việc theo chế độ kiêm nhiệm, tự giải thể khi hoàn thành nhiệm vụ. Căn cứ tính chất, vai trò của hệ thống thông tin, thành viên Hội

đồng thẩm định có thể bao gồm Bộ Công an, Bộ Quốc phòng, Bộ Thông tin và Truyền thông, Ban Cơ yếu Chính phủ và các cơ quan, đơn vị có liên quan. Tùy từng trường hợp cụ thể, Hội đồng thẩm định mời chủ quản hệ thống thông tin tham dự họp thẩm định;

c) Hội đồng thẩm định có trách nhiệm thẩm định cấp độ an toàn hệ thống thông tin và hồ sơ đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

5. Kết quả họp Hội đồng thẩm định được sử dụng chung phục vụ công tác an ninh mạng, an toàn thông tin mạng.

6. Trường hợp cần xác thực thông tin trong hồ sơ và hiện trạng thực tế của hệ thống thông tin được nêu trong hồ sơ, cơ quan thẩm định quy định tại khoản 1, khoản 2, khoản 3 Điều này tổ chức khảo sát, kiểm tra thực tế để thẩm định đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia. Thời gian khảo sát, kiểm tra thực tế không quá 20 ngày.

Kết quả khảo sát được lập thành biên bản có xác nhận của cơ quan thẩm định và chủ quản hệ thống thông tin.

7. Chủ quản hệ thống thông tin có trách nhiệm phối hợp, tạo điều kiện cho công tác thẩm định, khảo sát, kiểm tra và bổ sung hồ sơ theo đề nghị của cơ quan thẩm định.

8. Thời gian, trình tự thẩm định hồ sơ:

a) Thời gian thẩm định hồ sơ là 30 ngày kể từ ngày nhận đủ hồ sơ hợp lệ đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia hoặc kết thúc quá trình khảo sát theo quy định tại khoản 6 Điều này;

b) Thời gian xác nhận hồ sơ hợp lệ là 03 ngày làm việc sau khi nhận đủ hồ sơ đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia;

c) Kết thúc thời gian thẩm định, cơ quan thẩm định hoàn tất hồ sơ đề xuất Bộ trưởng Bộ Công an, Bộ trưởng Bộ Quốc phòng trình Thủ tướng Chính phủ ban hành, cập nhật quyết định theo chức năng, nhiệm vụ được giao. Đồng thời, có văn bản thông báo kết quả thẩm định cho chủ quản hệ thống thông tin (Mẫu số 04 Phụ lục);

d) Bộ trưởng Bộ Công an, Bộ trưởng Bộ Quốc phòng quyết định gia hạn thời gian thẩm định. Thời gian gia hạn không quá 20 ngày.

9. Bộ Công an chủ trì, phối hợp với Bộ Quốc phòng, Ban Cơ yếu Chính phủ thống nhất cơ chế trình Thủ tướng Chính phủ ban hành Quyết định xác lập, cập nhật Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

Điều 6. Đưa hệ thống thông tin ra khỏi danh mục hệ thống thông tin quan trọng về an ninh quốc gia

1. Khi xét thấy hệ thống thông tin quan trọng về an ninh quốc gia do mình quản lý không còn đáp ứng căn cứ quy định tại Điều 3 Nghị định này, chủ quản hệ thống thông tin quan trọng về an ninh quốc gia lập hồ sơ đề nghị đưa hệ thống thông tin ra khỏi Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

2. Hằng năm, lực lượng chuyên trách bảo vệ an ninh mạng căn cứ chức năng, nhiệm vụ rà soát các hệ thống thông tin không còn tiêu chí phù hợp với quy định tại Điều 3 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 ra khỏi Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

3. Hồ sơ đề nghị đưa hệ thống thông tin ra khỏi Danh mục hệ thống thông tin quan trọng về an ninh quốc gia, bao gồm:

a) Văn bản đề nghị đưa hệ thống thông tin ra khỏi Danh mục hệ thống thông tin quan trọng về an ninh quốc gia (Mẫu số 05 Phụ lục);

b) Văn bản, tài liệu cần thiết khác có liên quan trực tiếp đến việc đề nghị đưa hệ thống thông tin ra khỏi Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

4. Trình tự, thủ tục, thẩm quyền xem xét, quyết định đưa hệ thống thông tin ra khỏi Danh mục hệ thống thông tin quan trọng về an ninh quốc gia được áp dụng theo quy định về trình tự, thủ tục, thẩm quyền xem xét, quyết định đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

Điều 7. Phối hợp thẩm định, đánh giá, kiểm tra, giám sát, ứng phó, khắc phục sự cố đối với hệ thống thông tin quan trọng về an ninh quốc gia

1. Việc bảo vệ an ninh mạng, an toàn thông tin mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia được thực hiện theo quy định của pháp luật về an ninh mạng, an toàn thông tin mạng.

2. Nguyên tắc phối hợp

a) Áp dụng quy định của pháp luật về an ninh mạng, an toàn thông tin mạng đối với thẩm định, đánh giá, kiểm tra, giám sát, ứng phó, khắc phục sự cố đối với hệ thống thông tin quan trọng về an ninh quốc gia;

b) Trường hợp cần có sự phối hợp của nhiều bên liên quan, Bộ Công an, Bộ Quốc phòng, Ban Cơ yếu Chính phủ căn cứ Luật An ninh mạng chủ trì, phối hợp với Bộ Thông tin và Truyền thông, các bộ, ngành có liên quan tổ chức thẩm định, đánh giá, kiểm tra, giám sát, ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia theo chức năng, nhiệm vụ được giao;

c) Quá trình phối hợp bảo đảm tuân thủ quy định của các điều ước quốc tế và các quy định của tổ chức quốc tế mà Việt Nam tham gia, Luật An ninh mạng và pháp luật có liên quan, chủ động, thường xuyên, kịp thời và đúng chức năng, nhiệm vụ, quyền hạn được giao.

3. Phương thức phối hợp

a) Bộ Công an gửi văn bản đề nghị các bộ, ngành có liên quan cử thành viên tham gia thẩm định, đánh giá, kiểm tra, giám sát, ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia;

b) Các bộ, ngành có liên quan có trách nhiệm cử thành viên tham gia đầy đủ các hoạt động trong quá trình thẩm định, đánh giá, kiểm tra, giám sát, ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia theo nội dung đề nghị;

c) Hồ sơ, văn bản tài liệu phục vụ thẩm định, đánh giá, kiểm tra, giám sát, ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia được Bộ Công an sao gửi tới thành viên tham gia theo quy định.

4. Việc phối hợp giám sát đối với hệ thống thông tin quan trọng về an ninh quốc gia phục vụ công tác bảo vệ an ninh mạng, an toàn thông tin mạng:

a) Các lực lượng chuyên trách bảo vệ an ninh mạng có trách nhiệm chia sẻ với nhau và với Cục An toàn thông tin, Bộ Thông tin và Truyền thông về dữ liệu giám sát an ninh mạng, an toàn thông tin mạng phục vụ thực hiện chức năng, nhiệm vụ được giao;

b) Trường hợp đã thực hiện giám sát an toàn thông tin mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, dữ liệu giám sát được chia sẻ, dùng chung phục vụ công tác bảo vệ an ninh mạng, an toàn thông tin mạng;

c) Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia có trách nhiệm bố trí mặt bằng, điều kiện kỹ thuật, thiết lập, kết nối hệ thống, thiết bị giám sát của lực lượng chuyên trách bảo vệ an ninh mạng vào hệ thống thông tin do mình quản lý nhằm phát hiện, cảnh báo sớm nguy cơ an ninh mạng.

Mục 2
ĐIỀU KIỆN AN NINH MẠNG ĐỐI VỚI HỆ THỐNG THÔNG TIN QUAN TRỌNG VỀ AN NINH QUỐC GIA

Điều 8. Điều kiện về quy định, quy trình, phương án bảo đảm an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

1. Căn cứ vào các quy định bảo vệ an ninh mạng, bảo vệ bí mật nhà nước, bí mật công tác, tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin mạng và các tiêu chuẩn kỹ thuật chuyên ngành khác có liên quan, chủ quản hệ thống thông tin quan trọng về an ninh quốc gia xây dựng các quy định, quy trình, phương án bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia do mình quản lý.

2. Nội dung các quy định, quy trình, phương án về bảo vệ an ninh mạng phải quy định rõ hệ thống thông tin và thông tin quan trọng cần ưu tiên bảo vệ; quy trình quản lý, kỹ thuật, nghiệp vụ trong sử dụng, bảo vệ an ninh mạng đối với dữ liệu, hạ tầng kỹ thuật; điều kiện về nhân sự làm công tác quản trị mạng, vận hành hệ thống, bảo đảm an ninh, an toàn thông tin mạng và hoạt động soạn thảo, lưu trữ, truyền đưa bí mật nhà nước qua hệ thống thông tin; trách nhiệm của từng bộ phận, cá nhân trong quản lý, vận hành, sử dụng; chế tài xử lý những hành vi vi phạm.

Điều 9. Điều kiện về nhân sự vận hành, quản trị hệ thống, bảo vệ an ninh mạng

1. Có bộ phận phụ trách về vận hành, quản trị hệ thống và bảo vệ an ninh mạng.

2. Nhân sự phụ trách về vận hành, quản trị hệ thống và bảo vệ an ninh mạng phải có trình độ chuyên môn về an ninh mạng, an toàn thông tin mạng, công nghệ thông tin; có cam kết bảo mật thông tin liên quan đến hệ thống thông tin quan trọng về an ninh quốc gia trong quá trình làm việc và sau khi nghỉ việc.

3. Có cơ chế hoạt động độc lập về chuyên môn giữa các bộ phận vận hành, quản trị, bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia.

Điều 10. Điều kiện bảo đảm an ninh mạng đối với thiết bị, phần cứng, phần mềm là thành phần hệ thống

1. Các thiết bị phần cứng là thành phần hệ thống phải được kiểm tra an ninh mạng để phát hiện điểm yếu, lỗ hổng bảo mật, mã độc, thiết bị thu phát, phần cứng

độc hại bảo đảm sự tương thích với các thành phần khác trong hệ thống thông tin quan trọng về an ninh quốc gia. Các thiết bị quản trị phải được cài đặt hệ điều hành, phần mềm sạch, có các lớp tường lửa bảo vệ. Hệ thống thông tin xử lý bí mật nhà nước không được kết nối với mạng Internet.

2. Sản phẩm đã được lực lượng chuyên trách bảo vệ an ninh mạng, an toàn thông tin mạng cảnh báo, thông báo nguy cơ gây mất an ninh mạng không được đưa vào sử dụng hoặc phải có biện pháp xử lý, khắc phục điểm yếu, lỗ hổng bảo mật, mã độc, phần cứng độc hại trước khi đưa vào sử dụng.

3. Dữ liệu, thông tin ở dạng số được xử lý, lưu trữ thông qua hệ thống thông tin thuộc bí mật nhà nước phải được mã hóa hoặc có biện pháp bảo vệ trong quá trình tạo lập, trao đổi, lưu trữ trên mạng Internet theo quy định của pháp luật về bảo vệ bí mật nhà nước.

4. Thiết bị công nghệ thông tin, phương tiện truyền thông, vật mang tin và các thiết bị phục vụ cho hoạt động của hệ thống thông tin phải được quản lý, tiêu hủy, sửa chữa theo quy định của pháp luật về bảo vệ bí mật nhà nước, quy định công tác của chủ quản hệ thống thông tin.

5. Phần mềm hệ thống, phần mềm tiện ích, phần mềm lớp giữa, cơ sở dữ liệu, chương trình ứng dụng, mã nguồn và công cụ phát triển định kỳ được rà soát và cập nhật các bản vá lỗi.

6. Thiết bị di động và các thiết bị có tính năng lưu trữ thông tin khi kết nối vào hệ thống mạng nội bộ của hệ thống thông tin quan trọng về an ninh quốc gia phải được kiểm tra, kiểm soát bảo đảm an toàn và chỉ được phép sử dụng tại hệ thống thông tin quan trọng về an ninh quốc gia.

7. Thiết bị, phương tiện lưu trữ thông tin khi kết nối, vận chuyển, lưu trữ phải:

a) Kiểm tra bảo mật trước khi kết nối với hệ thống thông tin quan trọng về an ninh quốc gia;

b) Kiểm soát việc đấu nối, gỡ bỏ đấu nối thiết bị thuộc hệ thống thông tin quan trọng về an ninh quốc gia;

c) Triển khai các biện pháp bảo đảm an toàn khi vận chuyển, lưu trữ và biện pháp bảo vệ đối với thông tin thuộc bí mật nhà nước được lưu trữ trong đó.

Điều 11. Điều kiện về biện pháp kỹ thuật để giám sát, bảo vệ an ninh mạng

1. Môi trường vận hành của hệ thống thông tin quan trọng về an ninh quốc gia phải đáp ứng yêu cầu:

a) Tách biệt với các môi trường phát triển, kiểm tra và thử nghiệm;

b) Áp dụng các giải pháp bảo đảm an toàn thông tin;

c) Không cài đặt các công cụ, phương tiện phát triển ứng dụng;

d) Loại bỏ hoặc tắt các tính năng, phần mềm tiện ích không sử dụng, không cần thiết trên hệ thống thông tin.

2. Dữ liệu của hệ thống thông tin quan trọng về an ninh quốc gia phải có phương án tự động sao lưu dự phòng phù hợp ra phương tiện lưu trữ ngoài với tần suất thay đổi của dữ liệu và bảo đảm nguyên tắc dữ liệu phát sinh phải được sao lưu trong vòng 24 giờ. Dữ liệu sao lưu dự phòng phải được kiểm tra, bảo đảm khả năng khôi phục định kỳ 6 tháng một lần.

3. Hệ thống mạng phải đáp ứng yêu cầu sau:

a) Chia tách thành các vùng mạng khác nhau theo đối tượng sử dụng, mục đích sử dụng, tối thiểu: có phân vùng mạng riêng cho máy chủ của hệ thống thông tin; có phân vùng mạng trung gian (DMZ) để cung cấp dịch vụ trên mạng Internet; có phân vùng mạng riêng để cung cấp dịch vụ mạng không dây; có phân vùng mạng riêng đối với máy chủ cơ sở dữ liệu;

b) Có thiết bị, phần mềm thực hiện chức năng kiểm soát các kết nối, truy cập vào ra các vùng mạng quan trọng;

c) Có giải pháp kiểm soát, phát hiện và ngăn chặn kịp thời các kết nối, truy cập không tin cậy, xâm nhập trái phép;

d) Có phương án ứng phó tấn công từ chối dịch vụ và các hình thức tấn công khác phù hợp với quy mô, tính chất của hệ thống thông tin quan trọng về an ninh quốc gia.

4. Có biện pháp, giải pháp để dò tìm và phát hiện kịp thời các điểm yếu, lỗ hổng về mặt kỹ thuật của hệ thống mạng và những kết nối, thiết bị, phần mềm cài đặt bất hợp pháp vào mạng.

5. Ghi và lưu trữ nhật ký về hoạt động của hệ thống thông tin và người sử dụng, các lỗi phát sinh, các sự cố an toàn thông tin tối thiểu 3 tháng theo hình thức tập trung và sao lưu tối thiểu một năm một lần.

6. Kiểm soát truy cập đối với người sử dụng, nhóm người sử dụng thiết bị công cụ sử dụng:

a) Đăng ký, cấp phát, gia hạn và thu hồi quyền truy cập của thiết bị, người sử dụng;

b) Mỗi tài khoản truy cập hệ thống phải được gán cho một người sử dụng duy nhất; trường hợp chia sẻ tài khoản dùng chung để truy cập hệ thống thông tin quan trọng về an ninh quốc gia thì phải được phê duyệt bởi cấp có thẩm quyền và xác định được trách nhiệm cá nhân tại mỗi thời điểm sử dụng;

c) Giới hạn và kiểm soát các truy cập sử dụng tài khoản có quyền quản trị: (i) Thiết lập cơ chế kiểm soát việc tạo tài khoản có quyền quản trị để bảo đảm không một tài khoản nào sử dụng được khi chưa được cấp có thẩm quyền phê duyệt; (ii) Phải có biện pháp giám sát việc sử dụng tài khoản có quyền quản trị; (iii) Việc sử dụng tài khoản có quyền quản trị phải được giới hạn đảm bảo chỉ có 1 truy cập quyền quản trị duy nhất, tự động thoát khỏi phiên đăng nhập khi không có hoạt động trong khoảng thời gian nhất định;

d) Quản lý, cấp phát mã khóa bí mật truy cập hệ thống thông tin;

đ) Rà soát, kiểm tra, xét duyệt lại quyền truy cập của người sử dụng;

e) Yêu cầu, điều kiện an toàn thông tin đối với các thiết bị, công cụ sử dụng để truy cập.

Điều 12. Điều kiện về an ninh vật lý

1. Hệ thống thông tin quan trọng về an ninh quốc gia được bố trí, lắp đặt tại các địa điểm an toàn và được bảo vệ để giảm thiểu những rủi ro trước các mối đe dọa, hiểm họa từ môi trường và xâm nhập trái phép.

2. Hệ thống thông tin quan trọng về an ninh quốc gia được bảo đảm về nguồn điện và các hệ thống hỗ trợ khi nguồn điện chính bị gián đoạn; có biện pháp chống quá tải hay sụt giảm điện áp, chống sét lan truyền; có hệ thống tiếp địa; có hệ thống máy phát điện dự phòng và hệ thống lưu điện bảo đảm thiết bị hoạt động liên tục.

3. Hệ thống thông tin quan trọng về an ninh quốc gia có phương án, biện pháp bảo vệ, chống sự xâm nhập thu thập thông tin của các thiết bị bay không người lái.

4. Trung tâm dữ liệu của hệ thống thông tin quan trọng về an ninh quốc gia được kiểm soát ra vào 24/7.

Chương III
TRÌNH TỰ, THỦ TỤC ÁP DỤNG MỘT SỐ BIỆN PHÁP BẢO VỆ AN NINH MẠNG

Điều 13. Trình tự, thủ tục thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

1. Thẩm định an ninh mạng đối với hệ thống thông tin thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia do lực lượng chuyên trách bảo vệ an ninh mạng thực hiện theo quy định.

2. Trình tự thực hiện thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

a) Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia nộp hồ sơ đề nghị thẩm định an ninh mạng cho lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền;

b) Lực lượng chuyên trách bảo vệ an ninh mạng tiếp nhận, kiểm tra, hướng dẫn hoàn thiện hồ sơ đề nghị thẩm định an ninh mạng và cấp giấy tiếp nhận ngay sau khi nhận đủ hồ sơ hợp lệ trong thời gian 03 ngày làm việc;

c) Lực lượng chuyên trách bảo vệ an ninh mạng tiến hành thẩm định an ninh mạng theo nội dung quy định tại khoản 3 Điều 11 Luật An ninh mạng và thông báo kết quả trong thời hạn 30 ngày, kể từ ngày cấp giấy tiếp nhận hồ sơ cho chủ quản hệ thống thông tin quan trọng về an ninh quốc gia.

3. Hồ sơ đề nghị thẩm định đối với hệ thống thông tin quan trọng về an ninh quốc gia, bao gồm:

a) Văn bản đề nghị thẩm định an ninh mạng (Mẫu số 06 Phụ lục);

b) Báo cáo nghiên cứu tiền khả thi, hồ sơ thiết kế thi công dự án đầu tư xây dựng hệ thống thông tin trước khi phê duyệt;

c) Đề án nâng cấp hệ thống thông tin trước khi phê duyệt trong trường hợp nâng cấp hệ thống thông tin quan trọng về an ninh quốc gia.

4. Trường hợp cần xác định sự phù hợp giữa hiện trạng của hệ thống thông tin quan trọng về an ninh quốc gia và hồ sơ đề nghị thẩm định, lực lượng chuyên trách bảo vệ an ninh mạng tiến hành khảo sát, đánh giá hiện trạng thực tế của hệ thống thông tin quan trọng về an ninh quốc gia để đối chiếu với hồ sơ đề nghị thẩm định. Việc khảo sát, đánh giá thực tế bảo đảm không gây ảnh hưởng tới hoạt động bình thường của chủ quản cũng như hệ thống thông tin quan trọng về an ninh quốc gia. Thời gian khảo sát, đánh giá thực tế không quá 07 ngày làm việc.

5. Kết quả thẩm định an ninh mạng được bảo vệ theo quy định của pháp luật.

Điều 14. Trình tự, thủ tục đánh giá điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

1. Đánh giá điều kiện an ninh mạng đối với hệ thống thông tin thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia do lực lượng chuyên trách bảo vệ an ninh mạng thực hiện theo quy định.

2. Trình tự đánh giá điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia:

a) Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia nộp hồ sơ đề nghị đánh giá điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia cho lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền đánh giá điều kiện an ninh mạng theo quy định tại khoản 3 Điều 12 Luật An ninh mạng;

b) Lực lượng chuyên trách bảo vệ an ninh mạng tiếp nhận, kiểm tra, hướng dẫn hoàn thiện hồ sơ đề nghị đánh giá điều kiện an ninh mạng và cấp giấy tiếp nhận ngay sau khi nhận đủ hồ sơ hợp lệ;

c) Sau khi tiếp nhận đủ hồ sơ hợp lệ, lực lượng chuyên trách bảo vệ an ninh mạng tiến hành đánh giá điều kiện an ninh mạng và thông báo kết quả trong thời hạn 30 ngày, kể từ ngày cấp giấy tiếp nhận đủ hồ sơ hợp lệ của chủ quản hệ thống thông tin quan trọng về an ninh quốc gia;

d) Trường hợp đủ điều kiện an ninh mạng, Thủ trưởng cơ quan đánh giá điều kiện an ninh mạng cấp Giấy chứng nhận đủ điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia trong vòng 03 ngày làm việc kể từ khi kết thúc đánh giá điều kiện an ninh mạng.

3. Hồ sơ đề nghị chứng nhận đủ điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia bao gồm:

a) Văn bản đề nghị chứng nhận điều kiện an ninh mạng (Mẫu số 07 Phụ lục);

b) Báo cáo nghiên cứu tiền khả thi, hồ sơ thiết kế thi công dự án đầu tư xây dựng hệ thống thông tin trước khi phê duyệt;

c) Hồ sơ giải pháp bảo đảm an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia.

4. Trường hợp không bảo đảm điều kiện an ninh mạng, lực lượng chuyên trách bảo vệ an ninh mạng yêu cầu chủ quản hệ thống thông tin quan trọng về an ninh quốc gia bổ sung, nâng cấp hệ thống thông tin quan trọng về an ninh quốc gia để bảo đảm đủ điều kiện.

Điều 15. Trình tự, thủ tục giám sát an ninh mạng

1. Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an, Bộ Tư lệnh Tác chiến Không gian mạng thuộc Bộ Quốc phòng có trách nhiệm thực hiện giám sát an ninh mạng đối với không gian mạng quốc gia, hệ thống

thông tin quan trọng về an ninh quốc gia theo chức năng, nhiệm vụ được giao. Ban Cơ yếu Chính phủ thực hiện giám sát an ninh mạng đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ theo chức năng, nhiệm vụ được giao.

2. Trình tự giám sát an ninh mạng của lực lượng chuyên trách bảo vệ an ninh mạng:

a) Gửi thông báo bằng văn bản yêu cầu triển khai biện pháp giám sát an ninh mạng tới chủ quản hệ thống thông tin; trong văn bản nêu rõ lý do, thời gian, nội dung và phạm vi tiến hành giám sát an ninh mạng;

b) Triển khai biện pháp giám sát an ninh mạng;

c) Định kỳ thống kê, báo cáo kết quả giám sát an ninh mạng.

3. Trách nhiệm của chủ quản hệ thống thông tin quan trọng về an ninh quốc gia:

a) Xây dựng, triển khai hệ thống giám sát an ninh mạng, phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thực hiện hoạt động giám sát an ninh mạng đối với hệ thống thông tin thuộc thẩm quyền quản lý;

b) Bố trí mặt bằng, điều kiện kỹ thuật, thiết lập, kết nối hệ thống, thiết bị giám sát của lực lượng chuyên trách bảo vệ an ninh mạng vào hệ thống thông tin do mình quản lý để phục vụ giám sát an ninh mạng;

c) Cung cấp và cập nhật thông tin về hệ thống thông tin thuộc thẩm quyền quản lý, phương án kỹ thuật triển khai hệ thống giám sát cho lực lượng chuyên trách bảo vệ an ninh mạng theo định kỳ hoặc đột xuất khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền;

d) Thông báo với lực lượng chuyên trách bảo vệ an ninh mạng về hoạt động giám sát của chủ quản hệ thống thông tin định kỳ 03 tháng một lần;

đ) Bảo mật các thông tin liên quan trong quá trình phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng.

4. Doanh nghiệp viễn thông, doanh nghiệp cung cấp dịch vụ công nghệ thông tin, viễn thông, internet có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng trong giám sát an ninh mạng theo thẩm quyền nhằm bảo vệ an ninh mạng.

5. Kết quả giám sát an ninh mạng được bảo mật theo quy định của pháp luật.

Điều 16. Trình tự, thủ tục kiểm tra an ninh mạng

1. Lực lượng chuyên trách bảo vệ an ninh mạng tiến hành kiểm tra an ninh mạng đối với hệ thống thông tin theo quy định tại khoản 5 Điều 13, khoản 1 Điều 24

Luật An ninh mạng. Nội dung kiểm tra an ninh mạng, bao gồm: kiểm tra việc tuân thủ các quy định của pháp luật về bảo đảm an ninh mạng, bảo vệ bí mật nhà nước trên không gian mạng; kiểm tra, đánh giá hiệu quả các phương án, biện pháp bảo đảm an ninh mạng, phương án, kế hoạch ứng phó, khắc phục sự cố an ninh mạng; kiểm tra, đánh giá phát hiện lỗ hổng, điểm yếu bảo mật, mã độc và tấn công thử nghiệm xâm nhập hệ thống; kiểm tra, đánh giá khác do chủ quản hệ thống thông tin quy định.

2. Trình tự, thủ tục kiểm tra an ninh mạng của lực lượng chuyên trách bảo vệ 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;

đ) Thông báo kết quả kiểm tra an ninh mạng trong 03 ngày làm việc kể từ ngày hoàn thành kiểm tra.

3. Trường hợp cần giữ nguyên hiện trạng hệ thống thông tin, phục vụ điều tra, xử lý hành vi vi phạm pháp luật, phát hiện điểm yếu, lỗ hổng bảo mật; 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 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.

Điều 17. Trình tự, thủ tục ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

1. Đối với các hệ thống thông tin quan trọng về an ninh quốc gia khi gặp sự cố an ninh mạng thì thực hiện trình tự, thủ tục ứng phó, khắc phục sự cố như sau:

a) Lực lượng chuyên trách bảo vệ an ninh mạng thông báo bằng văn bản và hướng dẫn biện pháp tạm thời để ngăn chặn, xử lý hoạt động tấn công mạng, khắc phục hậu quả do tấn công mạng, sự cố an ninh mạng cho chủ quản hệ thống thông tin quan trọng về an ninh quốc gia.

Trường hợp khẩn cấp, thông báo bằng điện thoại hoặc các hình thức khác trước khi thông báo bằng văn bản;

b) Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia có trách nhiệm thực hiện các biện pháp theo hướng dẫn và các biện pháp phù hợp khác để ngăn chặn, xử lý, khắc phục hậu quả ngay sau khi nhận được thông báo, trừ quy định tại điểm c khoản này.

Trường hợp vượt quá khả năng xử lý, kịp thời thông báo cho lực lượng chuyên trách bảo vệ an ninh mạng để điều phối, ứng phó khắc phục sự cố an ninh mạng;

c) Trường hợp cần ứng phó ngay để ngăn chặn hậu quả xảy ra có khả năng gây nguy hại cho an ninh quốc gia, lực lượng chuyên trách bảo vệ an ninh mạng quyết định trực tiếp điều phối, ứng phó khắc phục sự cố an ninh mạng.

2. Điều phối, ứng phó khắc phục sự cố an ninh mạng của lực lượng chuyên trách bảo vệ an ninh mạng:

a) Đánh giá, quyết định phương án ứng phó, khắc phục sự cố an ninh mạng;

b) Điều hành công tác ứng phó, khắc phục sự cố an ninh mạng;

c) Chủ trì tiếp nhận, thu thập, xử lý, trao đổi thông tin về ứng phó, khắc phục sự cố an ninh mạng;

d) Huy động, phối hợp với các tổ chức, cá nhân trong và ngoài nước có liên quan tham gia ứng phó, khắc phục sự cố an ninh mạng trong trường hợp cần thiết;

đ) Chỉ định đơn vị đầu mối phối hợp với các đơn vị chức năng của các quốc gia khác hoặc các tổ chức quốc tế trong hoạt động ứng phó, xử lý các sự cố liên quốc gia trên cơ sở thỏa thuận quốc tế hoặc điều ước quốc tế mà Việt Nam là thành viên;

e) Kiểm tra, giám sát, đôn đốc việc thực hiện của các đơn vị liên quan ứng phó, khắc phục sự cố an ninh mạng;

g) Lập biên bản quá trình ứng cứu sự cố an ninh mạng.

3. Tổ chức, cá nhân tham gia ứng phó, khắc phục sự cố an ninh mạng có trách nhiệm thực hiện các biện pháp, hoạt động ứng phó, khắc phục sự cố theo sự điều phối của lực lượng chuyên trách bảo vệ an ninh mạng.

4. Trường hợp bảo vệ an ninh quốc gia, trật tự an toàn xã hội, doanh nghiệp viễn thông, doanh nghiệp cung cấp dịch vụ Internet bố trí mặt bằng, cổng kết nối và các biện pháp kỹ thuật cần thiết để Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an thực hiện nhiệm vụ bảo đảm an ninh mạng. Thủ tục, quy trình cụ thể, doanh nghiệp viễn thông, doanh nghiệp cung cấp dịch vụ Internet phối hợp với Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an thực hiện.

Điều 18. Trình tự, thủ tục thực hiện biện pháp sử dụng mật mã để bảo vệ thông tin mạng

1. Lực lượng chuyên trách bảo vệ an ninh mạng sử dụng các biện pháp mã hóa bằng mật mã của cơ yếu để bảo vệ thông tin mạng khi truyền đưa thông tin, tài liệu có nội dung thuộc bí mật nhà nước trên không gian mạng. Các biện pháp mã hóa phải bảo đảm các yêu cầu theo quy định của pháp luật về cơ yếu, bảo vệ bí mật nhà nước, an ninh mạng.

2. Trường hợp cần thiết vì lý do an ninh quốc gia, trật tự an toàn xã hội, bảo vệ quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân, lực lượng chuyên trách bảo vệ an ninh mạng gửi văn bản yêu cầu các cơ quan, tổ chức, cá nhân có liên quan thực hiện mã hóa các thông tin không nằm trong phạm vi bí mật nhà nước trước khi tiến hành lưu trữ, truyền đưa trên mạng Internet. Nội dung văn bản phải nêu rõ lý do yêu cầu, nội dung cần mã hóa.

Điều 19. Trình tự, thủ tục thực hiện biện pháp yêu cầu xóa bỏ thông tin trái pháp luật hoặc thông tin sai sự thật trên không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân

1. Trường hợp áp dụng biện pháp:

a) Khi thông tin trên không gian mạng được cơ quan có thẩm quyền xác định là có nội dung xâm phạm an ninh quốc gia, tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng theo quy định của pháp luật;

b) Khi có căn cứ pháp luật xác định thông tin trên không gian mạng có nội dung làm nhục, vu khống; xâm phạm trật tự quản lý kinh tế; bịa đặt, sai sự thật gây hoang mang trong nhân dân, gây thiệt hại nghiêm trọng cho hoạt động kinh tế - xã hội đến mức phải yêu cầu xóa bỏ thông tin;

c) Các thông tin trên không gian mạng khác có nội dung được quy định tại điểm c, điểm đ, điểm e khoản 1 Điều 8 Luật An ninh mạng theo quy định của pháp luật.

2. Cục trưởng Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an, Thủ trưởng cơ quan có thẩm quyền của Bộ Thông tin và Truyền thông:

a) Quyết định áp dụng biện pháp yêu cầu xóa bỏ thông tin trái pháp luật hoặc thông tin sai sự thật trên không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân theo quy định tại khoản 1 Điều này;

b) Gửi văn bản yêu cầu các doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, dịch vụ trên mạng Internet, dịch vụ gia tăng trên không gian mạng, chủ quản hệ thống thông tin xóa bỏ thông tin trái pháp luật hoặc thông tin sai sự thật trên không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân theo quy định tại khoản 1 Điều này;

c) Kiểm tra việc chấp hành thực hiện biện pháp của các chủ thể có liên quan được yêu cầu;

d) Trao đổi, chia sẻ thông tin về việc thực hiện biện pháp này, trừ trường hợp nội dung thuộc phạm vi bí mật nhà nước hoặc yêu cầu nghiệp vụ của Bộ Công an.

3. Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng quyết định áp dụng biện pháp yêu cầu xóa bỏ thông tin trái pháp luật hoặc thông tin sai sự thật trên không gian mạng xâm phạm an ninh quốc gia, an ninh quân đội theo quy định tại khoản 1 Điều này đối với hệ thống thông tin quân sự.

Điều 20. Trình tự, thủ tục thực hiện biện pháp thu thập dữ liệu điện tử liên quan đến hoạt động xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng

1. Dữ liệu điện tử là thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự.

2. Cục trưởng Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an quyết định tiến hành biện pháp thu thập dữ liệu điện tử để phục vụ điều tra, xử lý các hành vi xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng.

3. Việc thu thập dữ liệu điện tử liên quan đến hoạt động xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng được thực hiện theo quy định của pháp luật; đồng thời bảo đảm các yêu cầu sau:

a) Giữ nguyên hiện trạng của thiết bị số, dữ liệu điện tử;

b) Việc sao ghi dữ liệu điện tử phải được thực hiện đúng quy trình bằng các thiết bị, phần mềm được công nhận, có thể kiểm chứng được, phải bảo vệ được tính nguyên vẹn của dữ liệu điện tử lưu trong thiết bị;

c) Quá trình khôi phục dữ liệu, tìm kiếm dữ liệu điện tử phải được ghi nhận lại bằng biên bản, hình ảnh, video, khi cần thiết có thể lặp lại quá trình đi tới kết quả tương tự để trình bày tại tòa án;

d) Người thực hiện thu thập dữ liệu điện tử phải là cán bộ chuyên trách được giao thực hiện nhiệm vụ thu thập dữ liệu điện tử.

4. Nguyên tắc sao chép, phục hồi dữ liệu điện tử liên quan đến hoạt động xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng:

a) Trường hợp dữ liệu điện tử được cho là có giá trị chứng minh tội phạm mà cần phải sao chép, phục hồi hoặc nếu muốn sao chép, phục hồi dữ liệu điện tử, người thực hiện sao chép, phục hồi phải có thẩm quyền để sao chép, phục hồi và phải quyết định của cấp có thẩm quyền theo quy định của pháp luật;

b) Lập biên bản cho các hoạt động sao chép, phục hồi chứng cứ điện tử, trường hợp cần thiết có thể mời một bên thứ ba độc lập tham gia, chứng kiến, xác nhận quy trình này.

5. Thu giữ phương tiện lưu trữ, truyền đưa, xử lý dữ liệu điện tử liên quan đến hoạt động xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng được thực hiện theo quy định pháp luật.

6. Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng quyết định áp dụng biện pháp thu thập dữ liệu điện tử để phục vụ điều tra các vụ việc vi phạm, tội phạm gây mất an ninh, an toàn thông tin, xâm phạm an ninh quốc gia, an ninh quân đội trên không gian mạng.

Điều 21. Trình tự, thủ tục thực hiện biện pháp đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin, thu hồi tên miền

1. Trường hợp áp dụng:

a) Có tài liệu chứng minh hoạt động của hệ thống thông tin là vi phạm pháp luật về an ninh quốc gia, an ninh mạng;

b) Hệ thống thông tin đang được sử dụng vào mục đích xâm phạm an ninh quốc gia, trật tự an toàn xã hội.

2. Bộ trưởng Bộ Công an trực tiếp quyết định đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin, tạm ngừng, thu hồi tên miền có hoạt động vi phạm pháp luật về an ninh mạng.

3. Cục trưởng Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an có trách nhiệm thực hiện quyết định đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin, tạm ngừng, thu hồi tên miền.

4. Trình tự, thủ tục thực hiện biện pháp:

a) Báo cáo về việc áp dụng biện pháp đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin, tạm ngừng, thu hồi tên miền;

b) Quyết định đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin, tạm ngừng, thu hồi tên miền;

c) Gửi văn bản yêu cầu các cơ quan, tổ chức, cá nhân có liên quan thực hiện đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin hoặc gửi Trung tâm Internet Việt Nam đề nghị tạm ngừng, thu hồi tên miền theo trình tự, thủ tục được pháp luật quy định; văn bản yêu cầu nêu rõ lý do, thời gian, nội dung và kiến nghị;

d) Trong trường hợp cấp bách, cần ngăn chặn kịp thời hoạt động của hệ thống thông tin tránh gây nguy hại cho an ninh quốc gia hoặc cần ngăn chặn hậu quả tác hại có thể xảy ra, Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an yêu cầu trực tiếp hoặc bằng văn bản qua fax, email để yêu cầu cơ quan, tổ chức, cá nhân đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin;

Trong thời gian chậm nhất là 24 giờ kể từ khi có yêu cầu, Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an phải gửi văn bản yêu cầu đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin. Trường hợp quá thời hạn trên mà không có quyết định bằng văn bản thì hệ thống thông tin được tiếp tục hoạt động. Tùy theo tính chất, mức độ, hậu quả xảy ra do việc chậm trễ gửi văn bản yêu cầu, cán bộ thực hiện và những người có liên quan phải chịu trách nhiệm theo quy định của pháp luật;

đ) Việc đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin phải được lập thành biên bản. Biên bản phải ghi rõ thời gian, địa điểm, căn cứ và được lập thành 02 bản. Cơ quan chức năng có thẩm quyền giữ một bản, cơ quan, tổ chức, cá nhân sở hữu, quản lý hệ thống thông tin giữ một bản;

e) Việc tạm ngừng, thu hồi tên miền quốc gia trong các trường hợp quy định tại khoản 1 Điều này, cơ quan chức năng có thẩm quyền gửi văn bản đề nghị Trung tâm Internet Việt Nam tạm ngừng, thu hồi tên miền theo trình tự, thủ tục được pháp luật quy định.

5. Việc đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin mà không có căn cứ được quy định tại khoản 2 Điều này thì Thủ trưởng,

Phó Thủ trưởng cơ quan chức năng có thẩm quyền và cán bộ có liên quan phải chịu trách nhiệm trước pháp luật, nếu gây thiệt hại cho cơ quan, tổ chức, cá nhân có liên quan thì phải bồi thường theo quy định của pháp luật.

Điều 22. Trách nhiệm của cơ quan, tổ chức, cá nhân trong triển khai các biện pháp bảo vệ an ninh mạng

1. Lực lượng chuyên trách bảo vệ an ninh mạng có trách nhiệm hướng dẫn cụ thể các cơ quan, tổ chức, cá nhân có liên quan thực hiện các quy định về trình tự, thủ tục áp dụng một số biện pháp bảo vệ an ninh mạng.

2. Các cơ quan, tổ chức, cá nhân trong phạm vi trách nhiệm, quyền hạn của mình, kịp thời phối hợp, hỗ trợ lực lượng chuyên trách bảo vệ an ninh mạng thực hiện các quy định về trình tự, thủ tục áp dụng một số biện pháp bảo vệ an ninh mạng.

3. Trường hợp doanh nghiệp cung cấp dịch vụ qua biên giới bị cơ quan có thẩm quyền công bố vi phạm pháp luật Việt Nam, tổ chức, doanh nghiệp Việt Nam có trách nhiệm phối hợp với cơ quan chức năng có thẩm quyền trong ngăn chặn, phòng ngừa, xử lý hành vi vi phạm pháp luật của các doanh nghiệp cung cấp dịch vụ qua biên giới.

4. Mọi hành vi lợi dụng hoặc lạm dụng các biện pháp bảo vệ an ninh mạng để vi phạm pháp luật thì tùy theo tính chất, mức độ vi phạm mà bị xử lý theo quy định của pháp luật; trường hợp gây thiệt hại đến quyền và lợi ích hợp pháp của tổ chức, cá nhân thì phải bồi thường theo quy định của pháp luật.

5. Đối với các hệ thống thông tin không nằm trong Danh mục hệ thống thông tin quan trọng về an ninh quốc gia, Bộ Công an, Bộ Quốc phòng, Bộ Thông tin và Truyền thông phối hợp đồng bộ bảo vệ an ninh mạng, bảo đảm an toàn thông tin mạng theo chức năng, nhiệm vụ được giao:

a) Bộ Thông tin và Truyền thông là đầu mối chủ trì đối với các hoạt động dân sự, trừ trường hợp quy định tại điểm b, c khoản này;

b) Bộ Công an là đầu mối chủ trì đối với các hoạt động bảo vệ an ninh quốc gia, trật tự an toàn xã hội, bảo vệ an ninh mạng, phòng, chống tội phạm mạng, khủng bố mạng, gián điệp mạng;

c) Bộ Quốc phòng là đầu mối chủ trì đối với các hoạt động bảo vệ tổ quốc trên không gian mạng.

Chương IV
TRIỂN KHAI MỘT SỐ HOẠT ĐỘNG BẢO VỆ AN NINH MẠNG TRONG CƠ QUAN NHÀ NƯỚC, TỔ CHỨC CHÍNH TRỊ Ở TRUNG ƯƠNG VÀ ĐỊA PHƯƠNG

Điều 23. Xây dựng, hoàn thiện quy định sử dụng mạng máy tính của cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương

1. Cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương phải xây dựng quy định sử dụng, quản lý và bảo đảm an ninh mạng máy tính nội bộ, mạng máy tính có kết nối mạng Internet do cơ quan, tổ chức mình quản lý. Nội dung các quy định về bảo đảm an toàn, an ninh mạng căn cứ vào những quy định về bảo vệ an ninh mạng, bảo vệ bí mật nhà nước, tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin mạng và các tiêu chuẩn kỹ thuật chuyên ngành khác có liên quan.

2. Quy định sử dụng, bảo đảm an ninh mạng máy tính của cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương phải bao gồm các nội dung cơ bản sau:

a) Xác định rõ hệ thống mạng thông tin và thông tin quan trọng cần ưu tiên bảo đảm an ninh mạng;

b) Quy định rõ các điều cấm và các nguyên tắc quản lý, sử dụng và bảo đảm an ninh mạng, mạng máy tính nội bộ có lưu trữ, truyền đưa bí mật nhà nước phải được tách biệt vật lý hoàn toàn với mạng máy tính, các thiết bị, phương tiện điện tử có kết nối mạng Internet, trường hợp khác phải bảo đảm quy định của pháp luật về bảo vệ bí mật nhà nước;

c) Quy trình quản lý, nghiệp vụ, kỹ thuật trong vận hành, sử dụng và bảo đảm an ninh mạng đối với dữ liệu, hạ tầng kỹ thuật, trong đó phải đáp ứng các yêu cầu cơ bản bảo đảm an toàn hệ thống thông tin;

d) Điều kiện về nhân sự làm công tác quản trị mạng, vận hành hệ thống, bảo đảm an ninh mạng, an toàn thông tin và liên quan đến hoạt động soạn thảo, lưu trữ, truyền đưa bí mật nhà nước qua hệ thống mạng máy tính;

đ) Quy định rõ trách nhiệm của từng bộ phận, cán bộ, nhân viên trong quản lý, sử dụng, bảo đảm an ninh mạng, an toàn thông tin;

e) Chế tài xử lý những vi phạm quy định về đảm bảo an ninh mạng.

Điều 24. Xây dựng, hoàn thiện phương án bảo đảm an ninh mạng đối với hệ thống thông tin của cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương

1. Người đứng đầu cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương có trách nhiệm ban hành phương án bảo đảm an ninh mạng đối với hệ thống thông tin do mình quản lý, bảo đảm đồng bộ, thống nhất, tập trung, có sự chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư trùng lặp.

2. Phương án bảo đảm an ninh mạng đối với hệ thống thông tin bao gồm:

a) Quy định bảo đảm an ninh mạng trong thiết kế, xây dựng hệ thống thông tin, đáp ứng yêu cầu cơ bản như yêu cầu quản lý, kỹ thuật, nghiệp vụ;

b) Thẩm định an ninh mạng;

c) Kiểm tra, đánh giá an ninh mạng;

d) Giám sát an ninh mạng;

đ) Dự phòng, ứng phó, khắc phục sự cố, tình huống nguy hiểm về an ninh mạng;

e) Quản lý rủi ro;

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

Điều 25. Phương án ứng phó, khắc phục sự cố an ninh mạng của cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương

1. Phương án ứng phó, khắc phục sự cố an ninh mạng bao gồm:

a) Phương án phòng ngừa, xử lý thông tin có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; làm nhục, vu khống; xâm phạm trật tự quản lý kinh tế bị đăng tải trên hệ thống thông tin;

b) Phương án phòng, chống gián điệp mạng; bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên hệ thống thông tin;

c) Phương án phòng, chống hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội;

d) Phương án phòng, chống tấn công mạng;

đ) Phương án phòng, chống khủng bố mạng;

e) Phương án phòng ngừa, xử lý tình huống nguy hiểm về an ninh mạng.

2. Nội dung phương án ứng phó, khắc phục sự cố an ninh mạng

a) Các quy định chung;

b) Đánh giá các nguy cơ, sự cố an ninh mạng;

c) Phương án ứng phó, khắc phục đối với một số tình huống cụ thể;

d) Nhiệm vụ, trách nhiệm của các cơ quan trong tổ chức, điều phối, xử lý, ứng phó, khắc phục sự cố;

đ) Huấn luyện, diễn tập, phòng ngừa sự cố, giám sát phát hiện, bảo đảm các điều kiện sẵn sàng đối phó, khắc phục sự cố;

e) Các giải pháp đảm bảo, tổ chức triển khai phương án, kế hoạch và kinh phí thực hiện.

Chương V
LƯU TRỮ DỮ LIỆU VÀ ĐẶT CHI NHÁNH HOẶC VĂN PHÒNG ĐẠI DIỆN TẠI VIỆT NAM

Điều 26. Lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam

1. Dữ liệu phải lưu trữ tại Việt Nam:

a) Dữ liệu về thông tin cá nhân của người sử dụng dịch vụ tại Việt Nam;

b) Dữ liệu do người sử dụng dịch vụ tại Việt Nam tạo ra: Tên tài khoản sử dụng dịch vụ, thời gian sử dụng dịch vụ, thông tin thẻ tín dụng, địa chỉ thư điện tử, địa chỉ mạng (IP) đăng nhập, đăng xuất gần nhất, số điện thoại đăng ký được gắn với tài khoản hoặc dữ liệu;

c) Dữ liệu về mối quan hệ của người sử dụng dịch vụ tại Việt Nam: bạn bè, nhóm mà người sử dụng kết nối hoặc tương tác.

2. Doanh nghiệp trong nước lưu trữ dữ liệu quy định tại khoản 1 Điều này tại Việt Nam.

3. Việc lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam của doanh nghiệp nước ngoài:

a) Doanh nghiệp nước ngoài có hoạt động kinh doanh tại Việt Nam thuộc một trong những lĩnh vực sau: Dịch vụ viễn thông; lưu trữ, chia sẻ dữ liệu trên không gian mạng; cung cấp tên miền quốc gia hoặc quốc tế cho người sử dụng dịch vụ tại Việt Nam; thương mại điện tử; thanh toán trực tuyến; trung gian thanh toán; dịch vụ

kết nối vận chuyển qua không gian mạng; mạng xã hội và truyền thông xã hội; trò chơi điện tử trên mạng; dịch vụ cung cấp, quản lý hoặc vận hành thông tin khác trên không gian mạng dưới dạng tin nhắn, cuộc gọi thoại, cuộc gọi video, thư điện tử, trò chuyện trực tuyến phải lưu trữ dữ liệu quy định tại khoản 1 Điều này và đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam trong trường hợp dịch vụ do doanh nghiệp cung cấp bị sử dụng thực hiện hành vi vi phạm pháp luật về an ninh mạng đã được Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an thông báo và có yêu cầu phối hợp, ngăn chặn, điều tra, xử lý bằng văn bản nhưng không chấp hành, chấp hành không đầy đủ hoặc ngăn chặn, cản trở, vô hiệu hóa, làm mất tác dụng của biện pháp bảo vệ an ninh mạng do lực lượng chuyên trách bảo vệ an ninh mạng thực hiện;

b) Trường hợp bất khả kháng mà việc chấp hành yêu cầu của pháp luật về an ninh mạng của doanh nghiệp nước ngoài không thể thực hiện, doanh nghiệp nước ngoài thông báo cho Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an trong vòng 03 ngày làm việc để kiểm tra tính xác thực của việc bất khả kháng. Trong trường hợp này, doanh nghiệp có thời gian 30 ngày làm việc để tìm phương án khắc phục.

4. Trường hợp dữ liệu do doanh nghiệp thu thập, khai thác, phân tích, xử lý không đầy đủ theo quy định tại khoản 1 Điều này, doanh nghiệp phối hợp với Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an để xác nhận và tiến hành lưu trữ các loại dữ liệu hiện đang thu thập, khai thác, phân tích, xử lý.

Trường hợp doanh nghiệp tiến hành thu thập, khai thác, phân tích, xử lý bổ sung các loại dữ liệu theo quy định tại khoản 1 Điều này, doanh nghiệp có trách nhiệm phối hợp với Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an để bổ sung vào danh sách dữ liệu phải lưu trữ tại Việt Nam.

5. Hình thức lưu trữ dữ liệu tại Việt Nam do doanh nghiệp quyết định.

6. Trình tự, thủ tục yêu cầu lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện của doanh nghiệp nước ngoài tại Việt Nam:

a) Bộ trưởng Bộ Công an ra quyết định yêu cầu lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam;

b) Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an thông báo, hướng dẫn, theo dõi, giám sát, đôn đốc doanh nghiệp thực

hiện yêu cầu lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam; đồng thời, thông báo cho các cơ quan liên quan để thực hiện chức năng quản lý nhà nước theo thẩm quyền;

c) Trong thời hạn 12 tháng kể từ ngày Bộ trưởng Bộ Công an ra quyết định, các doanh nghiệp quy định tại điểm a khoản 3 Điều 26 của Nghị định này phải hoàn thành lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam.

7. Trình tự, thủ tục đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam được thực hiện theo các quy định của pháp luật về kinh doanh, thương mại, doanh nghiệp và các quy định khác có liên quan.

8. Các doanh nghiệp không chấp hành quy định tại Điều này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý theo quy định của pháp luật.

Điều 27. Thời gian lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam

1. Thời gian lưu trữ dữ liệu theo quy định tại Điều 26 Nghị định này bắt đầu từ khi doanh nghiệp nhận được yêu cầu lưu trữ dữ liệu đến khi kết thúc yêu cầu. Thời gian lưu trữ tối thiểu là 24 tháng.

2. Thời gian đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam theo quy định tại Điều 26 Nghị định này bắt đầu từ khi doanh nghiệp nhận được yêu cầu đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam đến khi doanh nghiệp không còn hoạt động tại Việt Nam hoặc dịch vụ được quy định không còn cung cấp tại Việt Nam.

3. Nhật ký hệ thống để phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng được quy định tại điểm b khoản 2 Điều 26 của Luật An ninh mạng được lưu trữ tối thiểu là 12 tháng.

Chương VI
ĐIỀU KHOẢN THI HÀNH

Điều 28. Kinh phí bảo đảm

1. Kinh phí thực hiện bảo đảm an ninh mạng trong hoạt động của cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương do ngân sách nhà nước bảo đảm.

2. Kinh phí đầu tư cho an ninh mạng sử dụng vốn đầu tư công thực hiện theo quy định của Luật Đầu tư công. Đối với dự án đầu tư công để xây dựng mới hoặc

mở rộng, nâng cấp hệ thống thông tin, kinh phí đầu tư được bố trí trong vốn đầu tư của dự án tương ứng.

3. Kinh phí thực hiện thẩm định, giám sát, kiểm tra, đánh giá điều kiện an ninh mạng; thực hiện các phương án bảo đảm an ninh mạng của cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương được cân đối, bố trí trong dự toán ngân sách hàng năm của cơ quan, tổ chức đó theo phân cấp của Luật Ngân sách nhà nước.

4. Bộ Tài chính hướng dẫn chi kinh phí phục vụ công tác bảo vệ an ninh mạng trong dự toán ngân sách, hướng dẫn quản lý và sử dụng kinh phí chi thường xuyên cho công tác bảo đảm an ninh mạng của cơ quan, tổ chức nhà nước.

5. Căn cứ nhiệm vụ được giao, cơ quan, tổ chức nhà nước thực hiện lập dự toán, quản lý, sử dụng và quyết toán kinh phí thực hiện nhiệm vụ bảo đảm an ninh mạng theo quy định của Luật Ngân sách nhà nước.

Điều 29. Hiệu lực thi hành

Nghị định này có hiệu lực từ ngày 01 tháng 10 năm 2022.

Điều 30. Trách nhiệm thi hành

1. Bộ trưởng Bộ Công an đôn đốc, kiểm tra, hướng dẫn việc thực hiện Nghị định này. Trong quá trình thực hiện, nếu có vướng mắc, các bộ, ngành, địa phương trao đổi Bộ Công an để tập hợp, báo cáo Chính phủ xem xét, quyết định, điều chỉnh.

2. Bộ trưởng, Thủ trưởng cơ quan ngang bộ, Thủ trưởng cơ quan thuộc Chính phủ, Chủ tịch Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương chịu trách nhiệm thi hành Nghị định này./.

TM. CHÍNH PHỦ
KT. THỦ TƯỚNG
PHÓ THỦ TƯỚNG

Vũ Đức Đam

Phụ lục

(Kèm theo Nghị định số 53/2022/NĐ-CP ngày 15 tháng 8 năm 2022 của Chính phủ)

Mẫu số 01	Văn bản đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia
Mẫu số 02	Văn bản cung cấp danh mục toàn bộ hệ thống thông tin của cơ quan, tổ chức
Mẫu số 03	Văn bản phản hồi tiếp nhận Hồ sơ đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia
Mẫu số 04	Văn bản thông báo ý kiến của Hội đồng thẩm định đối với hồ sơ đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia
Mẫu số 05	Văn bản đề nghị đưa hệ thống thông tin ra khỏi Danh mục hệ thống thông tin quan trọng về an ninh quốc gia
Mẫu số 06	Văn bản thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia
Mẫu số 07	Văn bản đề nghị chứng nhận điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

Mẫu số 01

CƠ QUAN, TỔ CHỨC	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số:... V/v đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia	*....., ngày... tháng... năm...*

Kính gửi:.....[1].

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

Căn cứ Nghị định số.../2022/NĐ-CP ngày... tháng... năm... của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng;

.....[2] đề nghị đưa hệ thống thông tin sau vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia:

1. Hệ thống thông tin đề nghị đưa vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia

a) Thông tin chung

- Tên hệ thống thông tin:

- Địa chỉ (nơi đặt hệ thông tin):

- Người phụ trách (*họ tên, chức vụ, số điện thoại, địa chỉ thư điện tử*):

b) Phạm vi, quy mô của hệ thống thông tin

- Tầm quan trọng:

- Mục đích sử dụng:

- Đối tượng phục vụ của hệ thống thông tin:

- Yêu cầu bảo vệ an ninh mạng:

2. Đơn vị chủ quản hệ thống thông tin

- Tên đơn vị:

- Văn bản quyết định thành lập/quy định chức năng, nhiệm vụ, quyền hạn:

- Người đại diện:

---

[1] Cơ quan thẩm định theo quy định tại khoản 1, khoản 2, khoản 3 Điều 5 của Nghị định này.

[2] Tên cơ quan, tổ chức.

- Địa chỉ:

- Thông tin liên hệ (*số điện thoại, địa chỉ thư điện tử*):

3. Đơn vị vận hành hệ thống thông tin

- Tên đơn vị:

- Văn bản quyết định thành lập/quy định chức năng, nhiệm vụ, quyền hạn:

- Người đại diện:

- Địa chỉ:

- Thông tin liên hệ (*số điện thoại, địa chỉ thư điện tử*):

4. Thuyết minh chi tiết sự phù hợp với căn cứ xác lập hệ thống thông tin quan trọng về an ninh quốc gia

a) Sự phù hợp với quy định tại khoản 2 Điều 10 Luật An ninh mạng (*nêu rõ căn cứ, lập luận chứng minh và các văn bản có liên quan*)

b) Sự phù hợp với quy định về hệ thống thông tin quan trọng quốc gia, công trình quan trọng liên quan đến an ninh quốc gia, công trình viễn thông quan trọng liên quan đến an ninh quốc gia (*nêu rõ căn cứ, lập luận chứng minh và các văn bản có liên quan*):

c) Đánh giá phạm vi, mức độ ảnh hưởng và xác định hậu quả của hệ thống thông tin khi bị sự cố, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại (*nêu rõ căn cứ, lập luận chứng minh và các văn bản có liên quan*).

5. Thuyết minh cấu trúc của hệ thống thông tin

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

b) Cấu trúc logic mô tả thiết kế các vùng mạng chức năng có trong hệ thống; hướng hết nối mạng; các thiết bị đầu cuối; các thiết bị mạng (*sơ đồ kết nối logic*).

c) Danh mục thiết bị sử dụng trong hệ thống (*thông tin tên thiết bị/chủng loại; vị trí triển khai, trường hợp thiết bị vật lý được chia thành các thiết bị logic thì vị trí triển khai là các vị trí của thiết bị logic; mục đích sử dụng*).

d) Danh mục các ứng dụng, dịch vụ trên hệ thống (*tên ứng dụng, dịch vụ; tên và cấu hình máy chủ/vị trí triển khai/hệ điều hành; mục đích sử dụng*).

đ) Danh mục đề xuất các thành phần, thiết bị mạng và mức độ quan trọng cần ưu tiên bảo vệ (*tên thiết bị, thông tin xử lý, chức năng/mức độ quan trọng*).

6. Thuyết minh phương án bảo đảm an ninh mạng về quản lý và kỹ thuật

a) Phương án bảo đảm an ninh mạng về quản lý (*nêu rõ phương án đã ban hành hoặc dự kiến ban hành, nội dung cơ bản, mục tiêu bảo vệ*).

b) Phương án bảo đảm an ninh mạng về kỹ thuật (*nêu rõ phương án đã ban hành hoặc dự kiến ban hành, nội dung cơ bản, mục tiêu bảo vệ*)

c) Phương án bảo đảm an ninh mạng về ứng phó, khắc phục sự cố an ninh mạng (*nêu rõ phương án đã ban hành hoặc dự kiến ban hành, nội dung cơ bản, mục tiêu bảo vệ*).

7. Tài liệu kèm theo

a) Danh mục thống kê toàn bộ hệ thống thông tin của cơ quan, tổ chức (*tên hệ thống thông tin, chức năng của hệ thống thông tin, mục đích sử dụng*).

b) Tài liệu thiết kế thi công đã được cấp có thẩm quyền phê duyệt hoặc tài liệu có giá trị tương đương (*trường hợp không có tài liệu thiết kế thi công, cần nêu rõ lý do*).

c) Các tài liệu khác là căn cứ được trích dẫn, nêu trong công văn này.

Nơi nhận:
- Như trên;
- .....

ĐẠI DIỆN CƠ QUAN, TỔ CHỨC
(Ký, ghi rõ họ tên, chức danh và đóng dấu)

Mẫu số 02

CƠ QUAN, TỔ CHỨC	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số:... V/v cung cấp danh mục toàn bộ hệ thống thông tin	*....., ngày... tháng... năm...*

Kính gửi:.....[1]

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

Căn cứ Nghị định số.../2022/NĐ-CP ngày... tháng... năm... của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng;

.....[2] cung cấp danh mục toàn bộ hệ thống thông tin hiện có như sau:

STT	Tên hệ thống thông tin	Đơn vị chủ quản	Địa chỉ	Thông tin liên hệ
1	Hệ thống thông tin A	- Tên đơn vị:		Người phụ trách (*họ tên, chức vụ, số điện thoại, địa chỉ thư điện tử*)

Nơi nhận:
- Như trên;
- .....

ĐẠI DIỆN CƠ QUAN, TỔ CHỨC
(Ký, ghi rõ họ tên, chức danh và đóng dấu)

[1] Cơ quan thẩm định theo quy định tại khoản 1, khoản 2, khoản 3 Điều 5 của Nghị định này.
[2] Tên cơ quan, đơn vị.

Mẫu số 03

CƠ QUAN, TỔ CHỨC[1]	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số:..... V/v tiếp nhận hồ sơ đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia	*....., ngày... tháng... năm...*

Kính gửi:.....[2]

....[3] nhận được công văn số..... ngày..... tháng..... năm..... của....[4] về việc đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia, như sau:

1. Thời gian nhận Hồ sơ đề nghị (*ghi rõ giờ, ngày, tháng, năm*):

.....

2. Hồ sơ đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia, gồm:...

.....

.....

Đề nghị bổ sung (*trường hợp hồ sơ chưa đầy đủ*):

.....

.....

Thời hạn bổ sung (*ghi ngày, tháng, năm*):

.....

3. Thời gian phản hồi ý kiến: dự kiến... giờ... ngày... tháng... năm...

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

[1] Cơ quan thẩm định theo quy định tại khoản 1, khoản 2, khoản 3 Điều 5 của Nghị định này.

[2] Cơ quan, đơn vị gửi hồ sơ đề nghị.

[3] Cơ quan tiếp nhận hồ sơ (cơ quan thẩm định theo quy định tại khoản 1, khoản 2, khoản 3 Điều 5 của Nghị định này).

[4] Cơ quan, đơn vị gửi hồ sơ đề nghị.

Mẫu số 04

CƠ QUAN, TỔ CHỨC[1]	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số:..... V/v thông báo ý kiến của Hội đồng thẩm định đối với hồ sơ đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia	*....., ngày... tháng... năm...*

Kính gửi:.....[2]

Ngày... tháng... năm..., Hội đồng thẩm định đã họp, cho ý kiến đối với Hồ sơ đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia của....[3], như sau:

1. Kết quả phiếu lấy ý kiến

STT	Tên hệ thống thông tin	Kết quả	
		Đạt	Chưa đạt
1		/	/

2. Kết luận

.....

.....

3. Đề nghị:

.....

.....

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

[1] Cơ quan thẩm định theo quy định tại khoản 1, khoản 2, khoản 3 Điều 5 của Nghị định này.
[2] Cơ quan, đơn vị gửi hồ sơ đề nghị.
[3] Cơ quan, đơn vị gửi hồ sơ đề nghị.

Mẫu số 05

CƠ QUAN, TỔ CHỨC	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số:..... V/v đề nghị đưa hệ thống thông tin ra khỏi Danh mục hệ thống thông tin quan trọng về an ninh quốc gia	*....., ngày... tháng... năm...*

Kính gửi:.....[1]

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

Căn cứ Nghị định số.../2022/NĐ-CP ngày... tháng... năm... của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng;

....[2] đề nghị đưa hệ thống thông tin sau ra khỏi Danh mục hệ thống thông tin quan trọng về an ninh quốc gia:

1. Thông tin chung

- Tên hệ thống thông tin:...

- Đơn vị chủ quản hệ thống thông tin:...

- Địa chỉ:...

- Quyết định đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia (*nêu rõ số, ngày tháng, trích yếu văn bản*):

2. Lý do

.....

3. Tài liệu kèm theo (*tài liệu chứng minh hệ thống thông tin không còn phù hợp là hệ thống thông tin quan trọng về an ninh quốc gia*)

.....

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

[1] Cơ quan thẩm định theo quy định tại khoản 1, khoản 2, khoản 3 Điều 5 của Nghị định này.
[2] Tên cơ quan, đơn vị.

Mẫu số 06

CƠ QUAN, TỔ CHỨC	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số:..... V/v thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia	*....., ngày... tháng... năm...*

Kính gửi:.....[1]

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

Căn cứ Nghị định số.../2022/NĐ-CP ngày... tháng... năm... của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng;

.....[2] đề nghị thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia:

1. Thông tin chung:

- Tên hệ thống thông tin:...

- Đơn vị chủ quản hệ thống thông tin:...

- Địa chỉ:...

- Quyết định đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia (*nêu rõ số, ngày tháng, trích yếu văn bản*):

2. Tài liệu kèm theo:

a) Báo cáo nghiên cứu tiền khả thi, hồ sơ thiết kế thi công dự án đầu tư xây dựng hệ thống thông tin trước khi phê duyệt;

b) Đề án nâng cấp hệ thống thông tin trước khi phê duyệt trong trường hợp nâng cấp hệ thống thông tin quan trọng về an ninh quốc gia.

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

[1] Cơ quan thẩm định theo quy định tại khoản 1, khoản 2, khoản 3 Điều 5 của Nghị định này.
[2] Tên cơ quan, đơn vị.

Mẫu số 07

CƠ QUAN, TỔ CHỨC	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số:..... V/v đề nghị chứng nhận điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia	*....., ngày... tháng... năm...*

Kính gửi:.....[1]

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

Căn cứ Nghị định số.../2022/NĐ-CP ngày... tháng... năm... của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng;

.....[2] đề nghị chứng nhận điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia:

1. Thông tin chung:

- Tên hệ thống thông tin:...

- Đơn vị chủ quản hệ thống thông tin:...

- Địa chỉ:...

- Quyết định đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia (*nêu rõ số, ngày tháng, trích yếu văn bản*):

2. Tài liệu kèm theo:

a) Báo cáo nghiên cứu tiền khả thi, hồ sơ thiết kế thi công dự án đầu tư xây dựng hệ thống thông tin trước khi phê duyệt;

b) Hồ sơ giải pháp bảo đảm an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia.

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

[1] Cơ quan thẩm định theo quy định tại khoản 1, khoản 2, khoản 3 Điều 5 của Nghị định này.

[2] Tên cơ quan, đơn vị.