

CHÍNH PHỦ

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập - Tự do - Hạnh phúc

Số:/2026/NĐ-CP

Hà Nội, ngày.....tháng.....năm 2026

DỰ THẢO 4

NGHỊ ĐỊNH

Quy định chi tiết một số điều và biện pháp thi hành Luật An ninh mạng

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

Căn cứ Luật An ninh quốc gia số 32/2004/QH11;

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 quy định chi tiết một số điều và biện pháp thi hành Luật An ninh mạng.

Chương I NHỮNG QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Nghị định này quy định chi tiết điểm a, b, c, d, đ, g, k, l, m khoản 1 Điều 5, khoản 4 Điều 25, khoản 5 Điều 34 Luật An ninh mạng và quy định cơ chế quản lý định danh địa chỉ IP đối với các doanh nghiệp cung cấp dịch vụ viễn thông, Internet.

Điều 2. Đối tượng áp dụng

Nghị định này áp dụng đối với cơ quan, tổ chức, cá nhân Việt Nam; cơ quan, tổ chức, cá nhân nước ngoài tại Việt Nam và người gốc Việt Nam chưa xác định được quốc tịch đang sinh sống tại Việt Nam đã được cấp giấy chứng nhận căn cước; cơ quan, tổ chức, cá nhân nước ngoài trực tiếp tham gia hoặc có liên quan đến hoạt động bảo vệ an ninh mạng tại Việt Nam.

Điều 3. Giải thích từ ngữ

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

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

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

3. *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 sự kết nối và tương tác của người sử dụng trên không gian mạng.



4. *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 chứa đựng dữ liệu cá nhân nhạy cảm do người sử dụng dịch vụ tại Việt Nam tạo ra.

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

6. *Dịch vụ trên mạng Internet* là dịch vụ Internet và dịch vụ nội dung thông tin trên mạng viễn thông di động theo quy định của pháp luật.

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

8. *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.

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

10. *Hành vi vi phạm pháp luật về an ninh thông tin mạng* là những hành vi của cá nhân, tổ chức sử dụng không gian mạng, hệ thống thông tin hoặc thiết bị số để thực hiện các hoạt động trái quy định của pháp luật quy định tại Điều 7 (Các hành vi bị nghiêm cấm về an ninh mạng) và Điều 13 (Các thông tin và hành vi sử dụng công nghệ thông tin, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng) Luật An ninh mạng 2025

11. *Chuyên ngành an ninh mạng* là các chuyên ngành đào tạo thuộc nhóm ngành an ninh mạng, an toàn thông tin, ngành an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao.

12. *Mật mã an ninh* là kỹ thuật mật mã và sản phẩm mật mã do Bộ Công an nghiên cứu, xây dựng, phát triển được sử dụng để bảo mật hoặc xác thực đối với dữ liệu thuộc phạm vi quản lý của Bộ Công an.

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

Điều 4. Nguyên tắc áp dụng biện pháp bảo vệ an ninh mạng

1. Việc áp dụng các biện pháp bảo vệ an ninh mạng phải tuân thủ quy định của Hiến pháp và pháp luật; bảo đảm lợi ích của Nhà nước, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

2. Các biện pháp bảo vệ an ninh mạng chỉ được áp dụng đúng mục đích, đúng đối tượng, đúng thẩm quyền và đúng trình tự, thủ tục theo quy định của pháp luật; chỉ được thực hiện sau khi có quyết định phê duyệt bằng văn bản của người có thẩm quyền.

Điều 5. Thẩm định an ninh mạng

1. Thẩm định an ninh mạng là việc cơ quan có thẩm quyền xem xét, đánh giá việc đáp ứng các yêu cầu về an ninh mạng đối với thiết kế, phương án triển khai, nâng cấp hệ thống thông tin quan trọng về an ninh quốc gia, làm căn cứ cho việc phê duyệt phương án bảo đảm an ninh mạng và là điều kiện bắt buộc trước khi hệ thống được chứng nhận đủ điều kiện về an ninh mạng để đưa vào vận hành, sử dụng.

2. Trường hợp kết quả xác định cấp độ an ninh mạng đã làm rõ yêu cầu, phạm vi và mức độ bảo đảm an ninh mạng đối với hệ thống thông tin thì cơ quan thẩm định an ninh mạng kế thừa, sử dụng các nội dung đã được đánh giá, kết luận và không thực hiện thẩm định lại các nội dung này, trừ trường hợp có thay đổi làm ảnh hưởng đến cấp độ an ninh mạng hoặc mức độ quan trọng về an ninh quốc gia của hệ thống thông tin.

3. Đối tượng thẩm định an ninh mạng, bao gồm:

a) Hồ sơ thiết kế chi tiết dự án đầu tư xây dựng mới, nâng cấp, mở rộng hệ thống thông tin trước khi phê duyệt;

b) Đề án, kế hoạch, phương án nâng cấp, mở rộng hệ thống thông tin trước khi phê duyệt.

4. Nội dung thẩm định an ninh mạng, bao gồm:

a) Việc tuân thủ các quy định, điều kiện về an ninh mạng trong thiết kế hệ thống thông tin;

b) Sự phù hợp của phương án bảo vệ, phương án ứng phó, khắc phục sự cố và bố trí nhân lực bảo vệ an ninh mạng.

5. Thẩm quyền thẩm định an ninh mạng:

a) Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an thực hiện thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, trừ trường hợp quy định tại điểm b và điểm c khoản này;

b) Bộ Tư lệnh Tác chiến không gian mạng thuộc Bộ Quốc phòng thực hiện thẩm định an ninh mạng đối với hệ thống thông tin quân sự;

c) Ban Cơ yếu Chính phủ thực hiện thẩm định an ninh mạng đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ.

Điều 6. Trình tự, thủ tục thẩm định an ninh mạng

1. Trình tự thực hiện thẩm định an ninh mạng:

a) Sau khi hệ thống thông tin đã được xác định cấp độ an ninh mạng theo quy định của pháp luật, chủ quản hệ thống thông tin nộp hồ sơ đề nghị thẩm định an ninh mạng đến cơ quan có thẩm quyền.

b) Cơ quan có thẩm quyền tiếp nhận, kiểm tra hồ sơ và cấp giấy tiếp nhận trong thời hạn 03 ngày làm việc kể từ ngày nhận đủ hồ sơ hợp lệ;

c) Cơ quan có thẩm quyền tổ chức thẩm định an ninh mạng và thông báo kết quả trong thời hạn 30 ngày kể từ ngày cấp giấy tiếp nhận hồ sơ.



2. Hồ sơ đề nghị thẩm định an ninh mạng, bao gồm:

- a) Văn bản đề nghị thẩm định an ninh mạng (Mẫu số 01 Phụ lục 1);
- b) Hồ sơ quy định tại khoản 3 Điều 5 Nghị định này.
- c) Tài liệu thể hiện kết quả xác định cấp độ an ninh mạng của hệ thống thông tin.

3. Trường hợp cần xác định sự phù hợp giữa hiện trạng của hệ thống thông tin và hồ sơ đề nghị thẩm định, cơ quan có thẩm quyền tiến hành khảo sát, đánh giá hiện trạng thực tế của hệ thống thông tin 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. Thời gian khảo sát, đánh giá thực tế không quá 07 ngày làm việc.

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

Điều 7. Đánh giá điều kiện an ninh mạng

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

2. Điều kiện an ninh mạng phải đáp ứng bao gồm:

- a) Quy định, quy trình, phương án bảo đảm an ninh mạng và nhân sự vận hành, quản trị hệ thống;
- b) Biện pháp bảo đảm an ninh mạng đối với trang thiết bị, phần cứng, phần mềm;
- c) Biện pháp kỹ thuật giám sát, bảo vệ an ninh mạng;
- d) Biện pháp bảo đảm an ninh vật lý, kiểm soát truy cập, chống rò rỉ dữ liệu.

3. Thẩm quyền đánh giá điều kiện an ninh mạng:

a) Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an thực hiện đánh giá, chứng nhận đủ điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, trừ trường hợp quy định tại điểm b và điểm c khoản này;

b) Bộ Tư lệnh Tác chiến không gian mạng thuộc Bộ Quốc phòng thực hiện đánh giá, chứng nhận đủ điều kiện an ninh mạng đối với hệ thống thông tin quân sự;

c) Ban Cơ yếu Chính phủ thực hiện đánh giá, chứng nhận đủ điều kiện an ninh mạng đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ.

4. Hệ thống thông tin quan trọng về an ninh quốc gia được đưa vào vận hành, sử dụng sau khi được chứng nhận đủ điều kiện an ninh mạng.

Điều 8. Trình tự, thủ tục đánh giá điều kiện an ninh mạng

1. Trình tự đánh giá điều kiện an ninh mạng:

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 cho cơ quan có thẩm quyền đánh giá điều kiện an ninh mạng theo quy định tại khoản 3 Điều 7 Nghị định này;

b) Cơ quan có thẩm quyền 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;

c) Sau khi tiếp nhận đủ hồ sơ hợp lệ, cơ quan có thẩm quyền 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;

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 trong vòng 03 ngày làm việc kể từ khi kết thúc đánh giá điều kiện an ninh mạng.

2. Hồ sơ đề nghị đánh giá điều kiện an ninh mạng đối với hệ thống thông tin bao gồm:

a) Văn bản đề nghị chứng nhận điều kiện an ninh mạng (Mẫu số 02 Phụ lục 2);

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.

3. Trường hợp không bảo đảm điều kiện an ninh mạng, cơ quan có thẩm quyền thông báo bằng văn bản và yêu cầu chủ quản hệ thống thông tin bổ sung, nâng cấp trước khi đưa vào vận hành.

Điều 9. Giám sát an ninh mạng đối với hệ thống thông tin

1. Giám sát an ninh mạng là hoạt động thu thập, phân tích thông tin nhằm phát hiện, cảnh báo sớm nguy cơ đe dọa an ninh mạng, sự cố an ninh mạng, điểm yếu, lỗ hổng bảo mật, mã độc, phần cứng độc hại để kịp thời phòng ngừa, xử lý và khắc phục.

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

a) Chủ trì tổ chức giám sát an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý;

b) Xây dựng cơ chế tự giám sát, tự cảnh báo và tiếp nhận cảnh báo về nguy cơ đe dọa an ninh mạng, sự cố an ninh mạng, điểm yếu, lỗ hổng bảo mật;

c) Đảm bảo hệ thống giám sát an ninh mạng, hệ thống phòng, chống mã độc tập trung có khả năng kết nối liên tục, chia sẻ dữ liệu cảnh báo nguy cơ, sự cố an ninh mạng đúng, đủ về Trung tâm An ninh mạng quốc gia của Bộ Công an hoặc Trung tâm An ninh mạng của tỉnh, thành phố để hỗ trợ giám sát an ninh mạng.

3. Đối với hệ thống thông tin quan trọng về an ninh quốc gia, chủ quản hệ thống thông tin có trách nhiệm phối hợp thường xuyên với lực lượng chuyên trách bảo vệ an ninh mạng trong việc tổ chức giám sát an ninh mạng theo yêu cầu bảo vệ an ninh quốc gia.

4. Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an thực hiện giám sát an ninh mạng đối với:

a) Không gian mạng quốc gia trừ hệ thống thông tin quân sự và hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ;

b) Hệ thống thông tin quan trọng về an ninh quốc gia theo chức năng, nhiệm vụ được giao;

c) Hệ thống thông tin của các cơ quan, tổ chức trong hệ thống chính trị theo chức năng, nhiệm vụ được giao;

d) Hệ thống thông tin khác trong trường hợp cần thiết theo quy định của Luật An ninh mạng.

5. Thông tin, tài liệu thu thập được từ hoạt động giám sát an ninh mạng được quản lý, bảo mật theo quy định của pháp luật.

Điều 10. Trình tự, thủ tục giám sát an ninh mạng

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

a) Thông báo bằng văn bản cho chủ quản hệ thống thông tin về việc triển khai biện pháp giám sát an ninh mạng, trong đó nêu rõ lý do, phạm vi, nội dung và thời gian giám sát, trừ trường hợp khẩn cấp nhằm bảo vệ an ninh quốc gia; trong trường hợp khẩn cấp không thể thông báo trước, phải có văn bản thông báo chính thức trong vòng 24 giờ sau khi triển khai biện pháp giám sát.

b) Triển khai các biện pháp kỹ thuật giám sát an ninh mạng theo phạm vi được thông báo;

c) Phân tích, đánh giá thông tin thu thập được, kịp thời cảnh báo nguy cơ, sự cố an ninh mạng;

d) Thông báo kịp thời cho chủ quản hệ thống thông tin về kết quả giám sát, nguy cơ, sự cố an ninh mạng phát hiện được; định kỳ hoặc đột xuất tổng hợp, báo cáo cơ quan có thẩm quyền theo quy định.

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

a) Phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng trong quá trình giám sát an ninh mạng;

b) Bảo đảm điều kiện kỹ thuật cần thiết phục vụ hoạt động giám sát an ninh mạng theo yêu cầu hợp pháp;

c) Cung cấp, cập nhật thông tin liên quan đến cấu hình, vận hành hệ thống thông tin khi có yêu cầu.

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

Điều 11. Kiểm tra an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

1. Kiểm tra an ninh mạng là hoạt động xác định thực trạng an ninh mạng của hệ thống thông tin, cơ sở hạ tầng hệ thống thông tin hoặc thông tin được lưu trữ, xử lý, truyền đưa trong hệ thống thông tin nhằm phòng ngừa, phát hiện, xử lý nguy cơ đe dọa an ninh mạng và đề xuất biện pháp bảo đảm hoạt động an toàn, liên tục của hệ thống thông tin.

2. Hệ thống thông tin quan trọng về an ninh quốc gia được kiểm tra an ninh mạng trong các trường hợp sau đây:

a) Khi đưa phương tiện điện tử, dịch vụ an ninh mạng vào sử dụng trong hệ thống thông tin;

b) Khi có thay đổi hiện trạng hệ thống thông tin;

c) Kiểm tra định kỳ hằng năm do chủ quản hệ thống thông tin thực hiện;

d) Kiểm tra an ninh mạng đột xuất khi xảy ra sự cố an ninh mạng, hành vi xâm phạm an ninh mạng; khi có yêu cầu quản lý nhà nước về an ninh mạng; hoặc khi hết thời hạn khắc phục điểm yếu, lỗ hổng bảo mật theo yêu cầu hoặc khuyến cáo của lực lượng chuyên trách bảo vệ an ninh mạng.

3. Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia có trách nhiệm:

a) Tổ chức tự kiểm tra an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý trong các trường hợp quy định tại các điểm a, b và c khoản 2 Điều này;

b) Thông báo kết quả kiểm tra an ninh mạng định kỳ bằng văn bản trước tháng 10 hằng năm cho lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền;

c) Phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng khi tiến hành kiểm tra an ninh mạng đột xuất.

4. Đối tượng kiểm tra an ninh mạng, bao gồm:

a) Hệ thống phần cứng, phần mềm, thiết bị số;

b) Quy định, quy trình, biện pháp bảo đảm an ninh mạng;

c) Thông tin được lưu trữ, xử lý, truyền đưa trong hệ thống thông tin;

d) Phương án ứng phó, khắc phục sự cố an ninh mạng;

đ) Biện pháp bảo vệ bí mật nhà nước và phòng, chống lộ, mất bí mật nhà nước qua các kênh kỹ thuật;

e) Nhân lực tham gia bảo vệ an ninh mạng.

5. Kiểm tra an ninh mạng đột xuất đối với hệ thống thông tin quan trọng về an ninh quốc gia do lực lượng chuyên trách bảo vệ an ninh mạng thực hiện theo thẩm quyền; việc thông báo, kết luận kiểm tra và yêu cầu khắc phục được thực hiện theo quy định của Nghị định này.

6. Kết quả kiểm tra an ninh mạng được bảo mật theo quy định của pháp luật.

Điều 12. 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 trong các trường hợp quy định tại Điều 11 của Nghị định này, trên cơ sở các căn cứ quy định tại Luật An ninh mạng.

2. Nội dung kiểm tra an ninh mạng, bao gồm:

a) 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;

b) Việc triển khai, duy trì và hiệu quả của các phương án, biện pháp bảo đảm an ninh mạng, phương án, kế hoạch ứng phó và khắc phục sự cố an ninh mạng;

c) Việc phát hiện, đánh giá điểm yếu, lỗ hổng bảo mật, mã độc và thử nghiệm khả năng xâm nhập hệ thống khi cần thiết;

d) Nội dung kiểm tra khác phù hợp với mục đích kiểm tra và tính chất của hệ thống thông tin theo quyết định của cơ quan kiểm tra hoặc theo đề nghị của chủ quản hệ thống thông tin.

3. Trình tự, thủ tục kiểm tra an ninh mạng, bao gồm:

a) Thông báo kế hoạch hoặc quyết định kiểm tra an ninh mạng theo quy định của pháp luật, trừ trường hợp kiểm tra đột xuất nhằm ngăn chặn kịp thời nguy cơ xâm hại an ninh quốc gia;

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

c) Tiến hành kiểm tra an ninh mạng, bảo đảm phối hợp với chủ quản hệ thống thông tin và không làm gián đoạn hoạt động bình thường của hệ thống, trừ trường hợp cần thiết để bảo vệ an ninh quốc gia;

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

đ) Thông báo kết quả kiểm tra an ninh mạng cho chủ quản hệ thống thông tin trong thời hạn 03 ngày làm việc kể từ ngày hoàn thành kiểm tra.

4. Trường hợp cần giữ nguyên hiện trạng hệ thống thông tin để phục vụ điều tra, xử lý vi phạm pháp luật, xác minh sự cố an ninh mạng hoặc khắc phục điểm yếu, lỗ hổng bảo mật, lực lượng chuyên trách bảo vệ an ninh mạng có văn bản yêu cầu chủ quản hệ thống thông tin tạm thời điều chỉnh hoặc tạm ngừng hoạt động kiểm tra an ninh mạng. Văn bản yêu cầu phải nêu rõ lý do, mục đích, phạm vi và thời hạn áp dụng.

Điều 13. Ứng phó, khắc phục sự cố an ninh mạng

1. Ứng phó, khắc phục sự cố an ninh mạng là tập hợp các hoạt động nhằm phát hiện, ngăn chặn, hạn chế, xử lý và khôi phục hệ thống thông tin khi xảy ra sự cố an ninh mạng.

2. Hoạt động ứng phó, khắc phục sự cố an ninh mạng bao gồm:

a) Phát hiện, xác định sự cố an ninh mạng;

b) Bảo vệ hiện trường, thu thập thông tin, chứng cứ;

c) Khoanh vùng, hạn chế phạm vi ảnh hưởng của sự cố;

- d) Phân tích, đánh giá, phân loại sự cố an ninh mạng;
- đ) Triển khai biện pháp ứng phó, khắc phục và khôi phục hệ thống;
- e) Xác minh nguyên nhân, truy tìm nguồn gốc sự cố;
- g) Điều tra, xử lý theo quy định của pháp luật.

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

- a) Xây dựng, triển khai, duy trì phương án ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý;
- b) Kịp thời triển khai phương án ứng phó, khắc phục khi xảy ra sự cố;
- c) Thông báo ngay cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an khi xác định sự cố an ninh mạng vượt quá khả năng xử lý hoặc xuất hiện tình huống nguy hiểm về an ninh mạng, trừ hệ thống thông tin quân sự và hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ;
- d) Báo cáo sự cố an ninh mạng với lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an, trừ trừ hệ thống thông tin quân sự và hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ.

4. Việc ứng phó, khắc phục sự cố an ninh mạng được thực hiện thông qua Mạng lưới ứng phó, khắc phục sự cố an ninh mạng quốc gia, hoạt động dưới sự điều phối thống nhất của Bộ Công an, bảo đảm sự phối hợp giữa lực lượng chuyên trách bảo vệ an ninh mạng, các bộ, ngành, địa phương và các cơ quan, tổ chức, doanh nghiệp có liên quan theo quy định của pháp luật.

Điều 14. Trình tự, thủ tục điều phối, ứng phó và khắc phục sự cố an ninh mạng

1. Khi xảy ra sự cố an ninh mạng, lực lượng chuyên trách bảo vệ an ninh mạng có trách nhiệm:

- a) Thông báo và hướng dẫn chủ quản hệ thống thông tin áp dụng biện pháp tạm thời để ngăn chặn, hạn chế thiệt hại;
- b) Trường hợp khẩn cấp, được áp dụng ngay các biện pháp điều phối, ứng phó cần thiết để bảo vệ an ninh quốc gia.

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

- a) Thực hiện các biện pháp ứng phó theo hướng dẫn của lực lượng chuyên trách bảo vệ an ninh mạng;
- b) Phối hợp, cung cấp thông tin, tạo điều kiện để lực lượng chuyên trách bảo vệ an ninh mạng thực hiện nhiệm vụ điều phối, ứng phó, khắc phục sự cố.

3. Lực lượng chuyên trách bảo vệ an ninh mạng thực hiện các nhiệm vụ điều phối, ứng phó, khắc phục sự cố an ninh mạng theo thẩm quyền, bao gồm:

- a) Đánh giá, quyết định phương án ứng phó;
- b) Điều hành, giám sát hoạt động ứng phó, khắc phục sự cố;

c) Huy động, phối hợp các cơ quan, tổ chức, cá nhân có liên quan trong và ngoài nước theo quy định của pháp luật;

d) Tổng hợp, báo cáo, đánh giá kết quả xử lý sự cố an ninh mạng.

4. Doanh nghiệp viễn thông, doanh nghiệp cung cấp dịch vụ Internet có trách nhiệm phối hợp, bố trí điều kiện kỹ thuật cần thiết để lực lượng chuyên trách bảo vệ an ninh mạng thực hiện nhiệm vụ bảo đảm an ninh mạng theo quy định của pháp luật.

Điều 15. 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 lưu trữ, truyền đưa thông tin, tài liệu có nội dung thuộc bí mật nhà nước trên không gian mạng. Việc sử dụng mật mã của cơ yếu phải tuân thủ quy định của pháp luật về cơ yếu, bảo vệ bí mật nhà nước và an ninh mạng.

2. Đối với dữ liệu, thông tin thuộc phạm vi quản lý của Bộ Công an, lực lượng chuyên trách bảo vệ an ninh mạng được sử dụng mật mã an ninh để thực hiện các biện pháp bảo mật hoặc xác thực dữ liệu nhằm phục vụ yêu cầu bảo vệ an ninh quốc gia, trật tự, an toàn xã hội và bảo đảm an ninh mạng.

3. 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. Văn bản yêu cầu phải nêu rõ lý do, phạm vi, nội dung thông tin cần mã hóa và biện pháp mã hóa áp dụng.

Điều 16. 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 khoản 2 Điều 7 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:

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 17. 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 ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự được tạo ra, lưu trữ, truyền đi hoặc nhận được bởi phương tiện điện tử.

2. Thẩm quyền quyết định tiến hành biện pháp thu thập dữ liệu điện tử:

a) 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;

b) Giám đốc Công an cấp tỉnh 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 thuộc phạm vi quản lý;

c) 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 toàn, an ninh, xâm phạm an ninh quốc gia, an ninh quân đội trên không gian mạng.

3. Hoạt động 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 pháp luật, đảm bảo các nguyên tắc, yêu cầu sau:

- a) Dữ liệu điện tử không bị can thiệp, làm thay đổi;
- b) Hoạt động thu thập dữ liệu phải được người có thẩm quyền quy định tại khoản 2 Điều này phê duyệt, thực hiện đúng quy trình, bằng các thiết bị, phần mềm được công nhận, có thể kiểm chứng được, đảm bảo tính nguyên vẹn của dữ liệu điện tử lưu trong phương tiện điện tử;
- c) Người thực hiện thu thập dữ liệu điện tử phải có đủ năng lực chuyên môn, được người có thẩm quyền quy định tại khoản 2 Điều này giao thực hiện nhiệm vụ thu thập dữ liệu điện tử theo quy định pháp luật;
- d) Quá trình thu thập dữ liệu điện tử phải được ghi nhận lại bằng biên bản, hình ảnh, khi cần thiết có thể lặp lại quá trình đi tới kết quả tương tự. Trường hợp cần thiết có thể mời một bên thứ ba độc lập tham gia chứng kiến, xác nhận quy trình này.

4. 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.

Điều 18. 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 Bộ Khoa học và Công nghệ (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 đề 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 trong các trường hợp quy định tại khoản 1 Điều này, cơ quan chức năng có thẩm quyền gửi văn bản đề nghị Bộ Khoa học và Công nghệ (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 19. 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 phối hợp đồng bộ bảo vệ an ninh mạng theo chức năng, nhiệm vụ được giao:

a) Bộ Công an là đầu mối chủ trì đối với các hoạt động dân sự, 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;

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

Chương III **BẢO ĐẢM AN NINH THÔNG TIN MẠNG**

Điều 20. Nguyên tắc bảo đảm an ninh thông tin mạng

1. Hoạt động bảo đảm an ninh thông tin mạng trong việc cung cấp dịch vụ trên mạng viễn thông, mạng Internet và các dịch vụ gia tăng trên không gian mạng tại Việt Nam phải bảo đảm chủ quyền quốc gia trên không gian mạng; bảo vệ an ninh quốc gia, trật tự, an toàn xã hội; bảo đảm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân theo quy định của pháp luật.

2. Việc áp dụng các biện pháp bảo đảm an ninh thông tin mạng phải được thực hiện đồng bộ về biện pháp quản lý nhà nước và kỹ thuật; phù hợp với tính chất, quy mô, phạm vi hoạt động của dịch vụ cung cấp của tổ chức, cá nhân và mức độ rủi ro đối với an ninh thông tin mạng.

3. Việc thu thập, lưu trữ, xử lý, sử dụng và cung cấp thông tin, dữ liệu trong quá trình cung cấp dịch vụ trên không gian mạng phải tuân thủ quy định của pháp luật về an ninh mạng, bảo vệ dữ liệu cá nhân và các quy định khác có liên quan của pháp luật Việt Nam.

Điều 21. Hoạt động bảo đảm an ninh thông tin mạng

1. Doanh nghiệp trong nước và doanh nghiệp nước ngoài khi cung cấp dịch vụ trên mạng viễn thông, mạng Internet và các dịch vụ gia tăng trên không gian mạng tại Việt Nam phải thực hiện các hoạt động bảo đảm an ninh thông tin mạng theo quy định tại Điều này và quy định khác có liên quan của pháp luật Việt Nam.

2. Hoạt động xác thực, bảo vệ thông tin và tài khoản người sử dụng dịch vụ bao gồm:

a) Thực hiện xác thực thông tin người sử dụng tại thời điểm đăng ký tài khoản số theo quy định của pháp luật;

b) Thực hiện xác thực tài khoản bằng số điện thoại di động tại Việt Nam; trường hợp người sử dụng không có số điện thoại di động tại Việt Nam thì thực hiện xác thực bằng số định danh cá nhân hoặc phương thức định danh điện tử hợp pháp khác theo quy định của pháp luật về định danh và xác thực điện tử;

c) Trường hợp người sử dụng dịch vụ dùng tính năng livestream nhằm mục đích thương mại thì phải thực hiện xác thực tài khoản bằng số định danh cá nhân theo quy định của pháp luật;

d) Áp dụng các biện pháp quản lý nhà nước, kỹ thuật cần thiết để bảo đảm an toàn, bảo mật thông tin và tài khoản của người sử dụng; chỉ cho phép các tài khoản đã được xác thực thực hiện việc đăng tải, chia sẻ thông tin và sử dụng các tính năng tương tác trên hệ thống.

3. Hoạt động cung cấp thông tin phục vụ bảo vệ an ninh thông tin mạng bao gồm:

a) Cung cấp thông tin người sử dụng dịch vụ cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an và Bộ Quốc phòng khi có yêu cầu hợp lệ, căn cứ theo quy định của pháp luật Việt Nam nhằm phục vụ công tác xác minh, điều tra, xử lý hành vi vi phạm pháp luật;

b) Việc yêu cầu và cung cấp thông tin được thực hiện bằng văn bản, phương tiện điện tử hoặc hình thức khác, bảo đảm xác thực chủ thể yêu cầu và bảo mật thông tin được cung cấp theo quy định của pháp luật;

c) Thời hạn cung cấp thông tin chậm nhất là 24 giờ kể từ thời điểm nhận được yêu cầu; trường hợp khẩn cấp đe dọa xâm hại an ninh quốc gia hoặc đe dọa tính mạng con người thì thời hạn cung cấp thông tin chậm nhất là 03 giờ.

4. Hoạt động ngăn chặn, xử lý thông tin, dịch vụ, ứng dụng vi phạm an ninh thông tin mạng bao gồm:

a) Hạn chế, ngăn chặn truy cập, xóa bỏ thông tin, gỡ bỏ dịch vụ, ứng dụng tại Việt Nam đối với nội dung vi phạm pháp luật về an ninh thông tin mạng khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an;

b) Thời hạn thực hiện yêu cầu chậm nhất là 24 giờ kể từ thời điểm nhận được yêu cầu; trường hợp khẩn cấp đe dọa xâm hại an ninh quốc gia thì thời hạn thực hiện chậm nhất là 06 giờ;

c) Áp dụng biện pháp quản lý nhà nước, kỹ thuật hạn chế, tạm ngừng hoặc ngừng cung cấp dịch vụ đối với tổ chức, cá nhân nhiều lần đăng tải thông tin vi phạm pháp luật về an ninh thông tin mạng theo yêu cầu của cơ quan có thẩm quyền và phù hợp với quy định của pháp luật.

d) Việc hạn chế hiển thị tại Việt Nam hoặc khóa tạm thời tài khoản cá nhân, trang, nhóm cộng đồng hoặc kênh nội dung được thực hiện trong các trường hợp sau đây:

- Trong thời hạn 30 ngày, đăng tải ít nhất 03 lần nội dung vi phạm pháp luật về an ninh thông tin mạng thì bị yêu cầu hạn chế hiển thị tại Việt Nam hoặc khóa tạm thời với thời hạn tối đa 60 ngày, tùy theo tính chất, mức độ vi phạm;

- Trong thời hạn 90 ngày, đăng tải ít nhất 10 lần nội dung vi phạm pháp luật về an ninh thông tin mạng thì bị yêu cầu hạn chế hiển thị tại Việt Nam hoặc khóa tạm thời với thời hạn tối đa 180 ngày, tùy theo tính chất, mức độ vi phạm;

đ) Việc hạn chế vĩnh viễn tại Việt Nam hoặc khóa vĩnh viễn tài khoản (ngăn chặn truy cập) được thực hiện trong các trường hợp sau đây:

- Đăng tải nội dung xâm phạm an ninh quốc gia của nước Cộng hòa xã hội chủ nghĩa Việt Nam;

- Đã bị khóa tạm thời từ 03 lần trở lên theo yêu cầu của cơ quan có thẩm quyền mà vẫn tiếp tục vi phạm;

- Đã bị xử phạt vi phạm hành chính nhưng tiếp tục tái phạm trong thời hạn 12 tháng kể từ ngày quyết định xử phạt có hiệu lực thi hành;

- Tài khoản của tổ chức, cá nhân đã bị cơ quan có thẩm quyền của Việt Nam ban hành quyết định khởi tố vụ án, khởi tố bị can hoặc đã bị Tòa án nhân dân ban hành bản án, quyết định có hiệu lực pháp luật.

5. Hoạt động tạm ngừng, ngừng cung cấp dịch vụ để bảo đảm an ninh thông tin mạng bao gồm việc không cung cấp hoặc tạm ngừng, ngừng cung cấp dịch vụ đối với tổ chức, cá nhân có hành vi đăng tải thông tin thuộc các trường hợp quy định tại các khoản 1, 2 và 3 Điều 13 và khoản 2 Điều 14 của Luật An ninh mạng khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an; việc tạm ngừng, ngừng cung cấp dịch vụ phải bảo đảm đúng phạm vi, đối tượng, thời hạn và phù hợp với quy định của pháp luật có liên quan.

6. Hoạt động lưu trữ và quản lý nhật ký hệ thống bao gồm:

a) Lưu trữ và quản lý nhật ký hệ thống phục vụ công tác quản lý nhà nước, bảo đảm an ninh thông tin mạng và xử lý hành vi vi phạm pháp luật;

b) Nhật ký hệ thống phải bao gồm tối thiểu các thông tin về tài khoản người sử dụng dịch vụ, thời gian đăng nhập, đăng xuất, địa chỉ IP đăng nhập, đăng xuất và nhật ký xử lý thông tin được đăng tải;

c) Thời gian lưu trữ nhật ký hệ thống phải đảm bảo có thể truy xuất dữ liệu ít nhất trong vòng 12 tháng và được thực hiện theo quy định của pháp luật và phải bảo đảm đáp ứng yêu cầu phục vụ công tác xác minh, điều tra, xử lý hành vi vi phạm pháp luật.

Điều 22. Biện pháp bảo đảm an ninh thông tin mạng

1. Biện pháp bảo đảm an ninh thông tin mạng bao gồm các biện pháp quản lý nhà nước, biện pháp kỹ thuật, biện pháp nghiệp vụ theo quy định của pháp luật.

2. Cơ quan nhà nước có thẩm quyền căn cứ vào tính chất, mức độ, phạm vi ảnh hưởng của nguy cơ, hành vi vi phạm để yêu cầu áp dụng một hoặc nhiều biện

pháp bảo đảm an ninh thông tin mạng đối với doanh nghiệp, tổ chức, cá nhân cung cấp và sử dụng dịch vụ trên không gian mạng.

3. Việc áp dụng biện pháp bảo đảm an ninh thông tin mạng phải bảo đảm tuân thủ nguyên tắc quy định tại Điều 20 của Nghị định này và không xâm phạm trái pháp luật quyền, lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

Điều 23. Trách nhiệm phối hợp trong bảo đảm an ninh thông tin mạng

1. Doanh nghiệp, tổ chức và cá nhân cung cấp, sử dụng dịch vụ trên không gian mạng có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng và cơ quan nhà nước có thẩm quyền trong việc triển khai các hoạt động, biện pháp bảo đảm an ninh thông tin mạng.

2. Cơ quan, tổ chức, cá nhân khi phát hiện hành vi vi phạm pháp luật về an ninh thông tin mạng có trách nhiệm thông báo, phối hợp với cơ quan có thẩm quyền theo quy định của pháp luật.

Điều 24. Lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện chịu trách nhiệm pháp lý tại Việt Nam

1. Dữ liệu phải lưu trữ tại Việt Nam:

a) Dữ liệu 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 chịu trách nhiệm pháp lý 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 dịch vụ đăng ký, duy trì tên miền 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; ứng dụng trực tuyến; 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 chịu trách nhiệm pháp lý 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 sau

03 lần và tối đa 06 tháng nhưng doanh nghiệp nước ngoài không có giải pháp khắc phục; không chấp hành; chấp hành không đầy đủ về phạm vi, số lượng từng vấn đề cần chấp hành trong văn bản yêu cầu 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, thông báo công khai cho người sử dụng và cập nhật danh sách dữ liệu phải lưu trữ tại Việt Nam.

5. Hình thức lưu trữ dữ liệu tại Việt Nam do doanh nghiệp tự quyết định, đảm bảo khả năng truy xuất, cung cấp kịp thời khi có yêu cầu của cơ quan có thẩm quyền và đảm bảo an toàn thông tin theo tiêu chuẩn, quy chuẩn kỹ thuật quốc gia.

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 này 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 25. 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 24 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 24 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 25 của Luật An ninh mạng được lưu trữ tối thiểu là 12 tháng.

CHƯƠNG IV QUẢN LÝ ĐỊNH DANH ĐỊA CHỈ IP

Điều 26. Nguyên tắc định danh địa chỉ IP

1. Việc quản lý định danh địa chỉ IP phải bảo đảm tính chính xác, toàn vẹn và khả năng truy nguyên duy nhất đối với tổ chức, cá nhân đăng ký sử dụng dịch vụ, địa chỉ lắp đặt đường truyền kết nối Internet đối với mạng băng thông rộng cố định, số điện thoại đăng ký đối với mạng viễn thông di động.

2. Doanh nghiệp cung cấp dịch vụ viễn thông, doanh nghiệp cung cấp dịch vụ Internet có trách nhiệm thiết lập, duy trì hệ thống kỹ thuật để ghi nhận, lưu trữ và quản lý thông tin phục vụ định danh địa chỉ IP gắn với thông tin thuê bao, thời điểm sử dụng dịch vụ và dịch vụ liên quan theo quy định của pháp luật.

3. Việc định danh địa chỉ IP được thực hiện xuyên suốt các giai đoạn cấp phát, sử dụng và thu hồi địa chỉ IP, bảo đảm tính liên tục, nhất quán và khả năng phục vụ yêu cầu quản lý nhà nước và các biện pháp bảo vệ an ninh mạng.

Điều 27. Nội dung, yêu cầu kỹ thuật định danh địa chỉ IP

1. Doanh nghiệp cung cấp dịch vụ viễn thông, Internet khi cấp phát địa chỉ IP cho tổ chức, cá nhân phải áp dụng biện pháp kỹ thuật để xác định chính xác danh tính thông tin thuê bao tại thời điểm cấp phát địa chỉ IP.

2. Dữ liệu nhật ký hệ thống cấp phát, quản lý địa chỉ IP được đồng bộ theo chuẩn thời gian quốc gia bao gồm tối thiểu các thông tin sau đây:

a) Địa chỉ IP nguồn, cổng nguồn, địa chỉ IP đích, cổng đích, giao thức kết nối;

b) Trong trường hợp sử dụng kỹ thuật dịch địa chỉ mạng (Network Address Translation) phải lưu trữ đầy đủ thông tin ánh xạ địa chỉ IP;

c) Thời điểm bắt đầu và thời điểm kết thúc phiên kết nối, được đồng bộ theo chuẩn thời gian quốc gia;

d) Mã định danh cổng cấp IP công cộng (Gateway ID); mã định danh phiên kết nối (Session ID);

đ) Thông tin thuê bao, tài khoản sử dụng địa chỉ IP tại thời điểm tương ứng;

3. Dữ liệu nhật ký hệ thống quy định tại khoản 2 Điều này phải được lưu trữ đầy đủ, liên tục tối thiểu 12 tháng; hệ thống lưu trữ dữ liệu phải bảo đảm tính toàn vẹn, an toàn, bảo mật, phòng ngừa việc sửa đổi, xóa bỏ và đảm bảo trích xuất, cung cấp dữ liệu cho lực lượng chuyên trách bảo vệ an ninh mạng để thực hiện biện pháp bảo vệ an ninh mạng theo thời gian thực.

Điều 28. Cung cấp thông tin định danh địa chỉ IP cho lực lượng chuyên trách bảo vệ an ninh mạng

1. Doanh nghiệp cung cấp dịch vụ viễn thông, Internet có trách nhiệm thiết lập, duy trì cơ chế kỹ thuật phù hợp đảm bảo khả năng kết nối, cung cấp thông tin phục vụ định danh địa chỉ IP với hệ thống kỹ thuật của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an theo quy định của pháp luật.

2. Đối với các yêu cầu cung cấp thông tin định danh địa chỉ IP cụ thể được thực hiện theo trình tự, thủ tục sau đây:

a) Trên cơ sở yêu cầu hợp pháp bằng văn bản hoặc yêu cầu điện tử hợp lệ của lực lượng chuyên trách bảo vệ an ninh mạng để thực hiện biện pháp bảo vệ an ninh mạng, xác minh, điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng;

b) Doanh nghiệp cung cấp dịch vụ viễn thông, Internet phải cung cấp đầy đủ, chính xác thông tin định danh địa chỉ IP (bao gồm: Họ tên cá nhân, thông tin tổ chức, số căn cước công dân, tên/mã thuê bao, địa chỉ đăng ký lắp đặt đường truyền kết nối Internet đối với mạng băng rộng cố định, số điện thoại đăng ký đối với mạng viễn thông di động) tại thời điểm tương ứng theo yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng;

c) Thời hạn cung cấp thông tin chậm nhất là 24 giờ kể từ thời điểm nhận được yêu cầu; đối với trường hợp khẩn cấp liên quan đến an ninh quốc gia, phòng, chống khủng bố mạng, tấn công mạng hoặc tội phạm đặc biệt nghiêm trọng, thời hạn cung cấp thông tin không quá 03 giờ.

3. Nghiêm cấm việc sử dụng, tiết lộ hoặc khai thác thông tin định danh địa chỉ IP vì mục đích thương mại, trừ trường hợp pháp luật có quy định khác.

Chương V **TẬP HUẤN KIẾN THỨC, KỸ NĂNG CHUYÊN SÂU** **VỀ AN NINH MẠNG**

Điều 29. Yêu cầu về kiến thức, kỹ năng chuyên sâu về an ninh mạng

1. Lực lượng bảo vệ an ninh mạng quy định tại điểm a và điểm b khoản 1 Điều 30 của Luật An ninh mạng và người trực tiếp quản trị, vận hành hệ thống thông tin cấp độ 3, cấp độ 4, cấp độ 5 trong cơ quan, tổ chức, doanh nghiệp nhà nước phải đáp ứng yêu cầu về kiến thức, kỹ năng chuyên sâu về an ninh mạng, trừ trường hợp đã được đào tạo chuyên ngành an ninh mạng hoặc được công nhận tương đương theo quy định.

2. Căn cứ vào vị trí việc làm, chức năng, nhiệm vụ được giao, các đối tượng quy định tại khoản 1 Điều này được xác định đáp ứng yêu cầu về kiến thức, kỹ năng chuyên sâu về an ninh mạng khi đáp ứng tối thiểu hai khối kiến thức, kỹ năng, bao gồm:

a) Khối kiến thức, kỹ năng nền tảng về an ninh mạng (áp dụng bắt buộc đối với mọi vị trí);

b) Ít nhất một khối kỹ năng chuyên sâu về an ninh mạng quy định tại khoản 4 Điều này.

3. Khối kiến thức, kỹ năng nền tảng về an ninh mạng bao gồm:

a) Kiến thức về pháp luật, chính sách, chiến lược về an ninh mạng, bao gồm Luật An ninh mạng và các văn bản hướng dẫn thi hành; quy định về bảo vệ dữ liệu cá nhân, bảo vệ bí mật nhà nước trên môi trường mạng; quyền, nghĩa vụ và trách nhiệm của cơ quan, tổ chức, cá nhân trong bảo vệ an ninh mạng; điều ước quốc tế về an ninh mạng mà Việt Nam là thành viên;

b) Kiến thức tổng quan về an ninh mạng, bao gồm khái niệm, phạm vi, đối tượng bảo vệ; các mối đe dọa an ninh mạng phổ biến; nguyên tắc bảo đảm an ninh mạng; kiến trúc bảo đảm an toàn hệ thống; tiêu chuẩn, chuẩn mực quốc tế và xu hướng phát triển công nghệ an ninh mạng.

4. Khối kỹ năng chuyên sâu về an ninh mạng được lựa chọn phù hợp với vị trí công tác, bao gồm một hoặc một số lĩnh vực sau đây:

- a) Quản trị, chính sách và pháp lý an ninh mạng;
- b) Ứng cứu, xử lý sự cố an ninh mạng và điều tra số;
- c) Kiểm tra, đánh giá điểm yếu, lỗ hổng an ninh mạng và an toàn phần mềm;
- d) Giám sát an ninh mạng, phân tích, cảnh báo sớm nguy cơ, mối đe dọa an ninh mạng;
- đ) Nghiên cứu, phát triển sản phẩm và hệ thống an ninh mạng;
- e) Thiết kế, kiến trúc an ninh mạng;
- g) Triển khai, vận hành và bảo đảm an ninh hệ thống thông tin;
- h) Bảo mật điện toán đám mây, hệ thống OT/IoT và công nghệ mới;
- i) Bảo mật dữ liệu, quyền riêng tư và quản lý thông tin.

5. Cá nhân có chứng chỉ chuyên môn về an ninh mạng do tổ chức nước ngoài cấp, còn hiệu lực và được Bộ Công an công nhận tương đương với khối kỹ năng

chuyên sâu quy định tại khoản 4 Điều này chỉ phải tham gia tập huấn khối kiến thức, kỹ năng nền tảng quy định tại khoản 3 Điều này.

6. Bộ Công an ban hành khung chương trình đào tạo, tập huấn tương ứng với từng chuẩn kiến thức, kỹ năng nền tảng và chuẩn kỹ năng chuyên sâu về an ninh mạng quy định tại Điều này, làm căn cứ thống nhất để tổ chức tập huấn, đánh giá kết quả và cấp chứng nhận trên phạm vi toàn quốc, trừ đối tượng thuộc phạm vi quản lý của Bộ Quốc phòng và Ban Cơ yếu Chính phủ.

7. Bộ Quốc phòng ban hành khung chương trình đào tạo, tập huấn tương ứng với từng chuẩn kiến thức, kỹ năng nền tảng và chuẩn kỹ năng chuyên sâu về an ninh mạng, làm căn cứ thống nhất để tổ chức tập huấn, đánh giá kết quả và cấp chứng nhận đối với lực lượng bảo vệ an ninh mạng thuộc phạm vi quản lý.

Điều 30. Tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng

1. Cơ sở được tổ chức hoạt động tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng cho các đối tượng quy định tại Điều 34 của Luật An ninh mạng khi đáp ứng đầy đủ các điều kiện sau đây:

a) Được thành lập và hoạt động hợp pháp theo quy định của pháp luật Việt Nam;

b) Có cơ sở vật chất, hạ tầng kỹ thuật, phòng học, phòng thực hành, hệ thống mô phỏng, diễn tập và tài liệu giảng dạy phù hợp với nội dung tập huấn;

c) Có đội ngũ giảng viên đáp ứng chuẩn kiến thức, kỹ năng chuyên sâu tương ứng với chuẩn kiến thức, kỹ năng quy định tại Điều 29 và đáp ứng yêu cầu tại Điều 32 của Nghị định này;

d) Có giáo trình, tài liệu, nội dung giảng dạy phù hợp với khung chương trình và chuẩn kiến thức, kỹ năng chuyên sâu về an ninh mạng.

2. Cơ sở tổ chức tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng có trách nhiệm:

a) Thông báo kế hoạch tổ chức khóa tập huấn (thời gian, địa điểm, nội dung, đối tượng) đến Bộ Công an chậm nhất 15 ngày trước ngày khai giảng;

b) Tổ chức tập huấn theo đúng khung chương trình, chuẩn kiến thức, kỹ năng; đánh giá kết quả và cấp chứng nhận theo quy định;

c) Lưu trữ hồ sơ, tài liệu liên quan đến khóa tập huấn trong thời hạn tối thiểu 05 năm; gửi báo cáo kết quả tập huấn về Bộ Công an trong thời hạn 30 ngày kể từ ngày kết thúc khóa học;

d) Cập nhật đầy đủ thông tin về cơ sở, học viên, giảng viên lên hệ thống quản lý theo quy định;

đ) Thực hiện chế độ báo cáo định kỳ hoặc đột xuất theo yêu cầu của cơ quan quản lý nhà nước về an ninh mạng.

3. Cơ sở tổ chức tập huấn có nhu cầu được Bộ Công an hướng dẫn, hỗ trợ về chương trình, nội dung, phương pháp tập huấn có thể đăng ký tham gia Mạng lưới

các cơ sở tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng do Bộ Công an quản lý.

4. Đối với các cơ sở đào tạo, tập huấn thuộc quản lý của Bộ Quốc phòng, thực hiện báo cáo theo quy định của Bộ Quốc phòng.

Điều 31. Mạng lưới các cơ sở tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng

1. Bộ Công an thành lập và quản lý Mạng lưới các cơ sở tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng nhằm:

- a) Hỗ trợ, hướng dẫn các cơ sở xây dựng chương trình, giáo trình, tài liệu tập huấn;
- b) Chia sẻ kinh nghiệm, tài liệu, công cụ phục vụ tập huấn;
- c) Tổ chức bồi dưỡng, nâng cao năng lực cho giảng viên;
- d) Giám sát, đánh giá chất lượng hoạt động tập huấn;
- đ) Tăng cường kết nối, phối hợp giữa các cơ sở tập huấn.

2. Cơ sở có nhu cầu tham gia Mạng lưới đăng ký với Bộ Công an; hồ sơ đăng ký bao gồm:

- a) Đơn đăng ký theo mẫu do Bộ Công an quy định;
- b) Tài liệu chứng minh việc thành lập và hoạt động hợp pháp;
- c) Thông tin về cơ sở vật chất, đội ngũ giảng viên và năng lực tổ chức tập huấn.

3. Bộ Công an xem xét hồ sơ và chấp thuận cho cơ sở tham gia Mạng lưới trong thời hạn 15 ngày làm việc kể từ ngày nhận đủ hồ sơ hợp lệ; việc chấp thuận tham gia Mạng lưới không phải là điều kiện bắt buộc để cơ sở được tổ chức tập huấn.

4. Cơ sở tham gia Mạng lưới được hưởng các quyền sau đây:

- a) Tiếp cận tài liệu, công cụ, nền tảng hỗ trợ tập huấn do Bộ Công an cung cấp;
- b) Tham gia các hoạt động bồi dưỡng, nâng cao năng lực do Bộ Công an tổ chức;
- c) Được hỗ trợ, hướng dẫn về chuyên môn, nghiệp vụ;
- d) Được giới thiệu trên cổng thông tin điện tử của Bộ Công an.

5. Cơ sở tham gia Mạng lưới có trách nhiệm:

- a) Tổ chức tập huấn đúng khung chương trình, chuẩn kiến thức, kỹ năng do Bộ Công an ban hành;
- b) Định kỳ báo cáo kết quả hoạt động tập huấn;
- c) Tham gia các hoạt động chung của Mạng lưới;
- d) Chấp hành việc kiểm tra, giám sát của Bộ Công an.

6. Cơ sở bị đình chỉ hoặc chấm dứt tham gia Mạng lưới trong các trường hợp sau đây:

- a) Vi phạm nghiêm trọng quy định về tổ chức tập huấn;
- b) Cấp chứng nhận không đúng quy định;
- c) Không thực hiện đầy đủ trách nhiệm của thành viên Mạng lưới;
- d) Có văn bản đề nghị rút khỏi Mạng lưới.

Điều 32. Yêu cầu đối với giảng viên tham gia tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng

1. Giảng viên tham gia giảng dạy, tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng phải có trình độ đại học trở lên thuộc các chuyên ngành an ninh mạng, công nghệ thông tin, điện tử - viễn thông hoặc chuyên ngành khác có liên quan, phù hợp với nội dung giảng dạy.

2. Giảng viên tham gia tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng phải đáp ứng một trong các điều kiện sau đây:

- a) Có ít nhất 03 năm kinh nghiệm thực tiễn trong lĩnh vực an ninh mạng;
- b) Có chứng chỉ chuyên môn, nghiệp vụ về an ninh mạng phù hợp với lĩnh vực giảng dạy.

3. Giảng viên tham gia tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng phải có năng lực sư phạm, kỹ năng truyền đạt kiến thức và hướng dẫn thực hành đáp ứng yêu cầu của hoạt động tập huấn.

Điều 33. Điều kiện cấp chứng nhận tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng

1. Cá nhân được cấp chứng nhận tập huấn khi đáp ứng đầy đủ các điều kiện sau đây:

- a) Tham dự tối thiểu 80% thời lượng của khóa tập huấn;
- b) Hoàn thành đầy đủ các bài tập, bài thực hành trong quá trình tập huấn;
- c) Đạt yêu cầu tại bài kiểm tra, đánh giá cuối khóa theo quy định.

2. Chứng nhận tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng:

- a) Do người đứng đầu cơ sở tổ chức tập huấn ký, đóng dấu;
- b) Ghi rõ họ, tên người được cấp chứng nhận; khối kiến thức, kỹ năng đã hoàn thành; thời gian tập huấn; ngày cấp;
- c) Có hiệu lực 02 năm kể từ ngày cấp.

3. Cơ sở tổ chức tập huấn có trách nhiệm gửi thông tin về chứng nhận đã cấp đến Bộ Công an để cập nhật, quản lý theo quy định. Đối với các cơ sở tổ chức tập huấn thuộc phạm vi quản lý của Bộ Quốc phòng, Ban Cơ yếu Chính phủ, việc gửi thông tin, quản lý chứng nhận thực hiện theo quy định của Bộ Quốc phòng và Ban Cơ yếu Chính phủ.

4. Cơ quan, tổ chức, doanh nghiệp nhà nước có trách nhiệm định kỳ rà soát, tổ chức, cử cán bộ tham gia cập nhật, bồi dưỡng kiến thức nhằm bảo đảm đáp ứng yêu cầu của vị trí công tác theo quy định tại khoản 1 Điều 29 của Nghị định này.

Chứng nhận tập huấn là một trong các tiêu chuẩn bắt buộc khi xét tuyển, bổ nhiệm hoặc giao nhiệm vụ cho các vị trí quy định tại khoản 1 Điều 29 của Nghị định này.

Điều 34. Trách nhiệm của Bộ Công an trong quản lý hoạt động tập huấn an ninh mạng

1. Ban hành khung chương trình, chuẩn kiến thức, kỹ năng chuyên sâu về an ninh mạng áp dụng thống nhất trên phạm vi toàn quốc.

2. Xây dựng, duy trì, cập nhật và quản lý cơ sở dữ liệu về cơ sở tập huấn, học viên và giảng viên tập huấn an ninh mạng.

3. Hướng dẫn chi tiết về chương trình, nội dung tập huấn; tiêu chuẩn, quy trình đánh giá kết quả học tập; mẫu chứng nhận tập huấn; quy trình đăng ký tham gia Mạng lưới; tiêu chuẩn cơ sở vật chất, trang thiết bị phục vụ tập huấn.

4. Tổ chức các hoạt động hỗ trợ, bồi dưỡng, nâng cao năng lực cho các cơ sở tập huấn và giảng viên.

5. Thực hiện kiểm tra, giám sát và xử lý vi phạm trong hoạt động tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng theo quy định của pháp luật.

Chương VI ĐIỀU KHOẢN THI HÀNH

Điều 35. Hiệu lực thi hành

1. Nghị định này có hiệu lực thi hành từ ngày 01 tháng 7 năm 2026.

2. Quy định về việc áp dụng các yêu cầu đối với kiến thức, kỹ năng chuyên sâu về an ninh mạng quy định tại Điều 29 của Nghị định này.

a) Cá nhân đang đảm nhiệm các vị trí quy định tại điểm a, điểm b khoản 1 Điều 30 của Luật An ninh mạng tại thời điểm Nghị định này có hiệu lực thi hành phải hoàn thành việc tập huấn và được cấp chứng nhận theo quy định trong thời hạn 18 tháng kể từ ngày Nghị định có hiệu lực;

b) Cơ quan, tổ chức, doanh nghiệp nhà nước có trách nhiệm xây dựng kế hoạch, bố trí kinh phí và tổ chức thực hiện việc tập huấn đối với cán bộ, công chức, viên chức thuộc đối tượng bắt buộc, bảo đảm phù hợp với lộ trình quy định; trong đó ưu tiên thực hiện theo thứ tự sau:

- Người quản trị, vận hành hệ thống thông tin cấp độ 5, cấp độ 4 phải hoàn thành việc tập huấn và được cấp chứng nhận theo quy định trong thời hạn 18 tháng kể từ ngày Nghị định có hiệu lực;

- Người quản trị, vận hành hệ thống thông tin cấp độ 3 phải hoàn thành việc tập

huấn và được cấp chứng nhận theo quy định trong thời hạn 24 tháng kể từ ngày Nghị định có hiệu lực.

3. Nghị định số 53/2022/NĐ-CP ngày 15 tháng 8 năm 2022 của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng hết hiệu lực kể từ ngày Nghị định này có hiệu lực thi hành.

Điều 36. Trách nhiệm thi hành

Bộ trưởng, Thủ trưởng cơ quan ngang Bộ, Thủ trưởng cơ quan thuộc Chính phủ, Chủ tịch Ủy ban nhân dân các tỉnh và các cơ quan, tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Nghị định này./.

Nơi nhận:

- Ban Bí thư Trung ương Đảng;
- Thủ tướng, các Phó Thủ tướng Chính phủ;
- Các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;
- HĐND, UBND các tỉnh, thành phố trực thuộc trung ương;
- Văn phòng Trung ương và các Ban của Đảng;
- Văn phòng Tổng Bí thư;
- Văn phòng Chủ tịch nước;
- Hội đồng Dân tộc và các Ủy ban của Quốc hội;
- Văn phòng Quốc hội;
- Tòa án nhân dân tối cao;
- Viện kiểm sát nhân dân tối cao;
- Kiểm toán Nhà nước;
- Ủy ban Trung ương Mặt trận Tổ quốc Việt Nam;
- Cơ quan Trung ương của các đoàn thể;
- VPCP: BTCN, các PCN, Trợ lý TTg, TGĐ Cổng TTĐT, các Vụ, Cục, đơn vị trực thuộc, Công báo;
- Lưu: VT, CDS (2b).

TM. CHÍNH PHỦ
THỦ TƯỚNG

PHỤ LỤC 1
DANH MỤC HỒ SƠ VÀ BIỂU MẪU
(Kèm theo Nghị định số.../2026/NĐ-CP ngày ... tháng ... năm 2026 của Chính phủ)

Mẫu số 01	Văn bản thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia
Mẫu số 02	Văn bản đề nghị chứng nhận điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia



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 số 116/2025/QH15;

Căn cứ Nghị định số .../2026/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 điểm a, b và c khoản 7 Điều 8 của Nghị
 định này.

² Tên cơ quan, đơn vị.

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 số 116/2025/QH15;
 Căn cứ Nghị định số .../2026/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 điểm a, b và c khoản 4 Điều 10 của Nghị định này.

² Tên cơ quan, đơn vị.

PHỤ LỤC 2
ĐIỀU KIỆN AN NINH MẠNG ĐỐI VỚI HỆ THỐNG THÔNG TIN
QUAN TRỌNG VỀ AN NINH QUỐC GIA
(Kèm theo Nghị định số...../2026/NĐ-CP ngày ... tháng ... năm 2026 của Chính phủ)

1. 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

a) 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 ninh 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.

b) 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 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.

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

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

b) 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, 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.

c) 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.

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

a) 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.

b) Sản phẩm đã được lực lượng chuyên trách bảo vệ an ninh 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.

c) 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.

d) 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.

đ) 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.

e) 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.

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

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

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

- 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.

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

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

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

- Áp dụng các giải pháp bảo đảm an ninh mạng;

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

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

b) 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.

c) Hệ thống mạng phải đáp ứng yêu cầu sau:

- 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;

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

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

- 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.

d) 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.

đ) 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 ninh mạng tối thiểu 3 tháng theo hình thức tập trung và sao lưu tối thiểu một năm một lần.

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

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

- 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;

- 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;

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

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

- Yêu cầu, điều kiện an ninh m đối với các thiết bị, công cụ sử dụng để truy cập.

5. Điều kiện về an ninh vật lý

a) 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.

b) 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.

c) 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.

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

