| CHÍNH PHỦ | CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM |
|---|---|
| | Độc lập - Tự do - Hạnh phúc |
| Số: 333/2026/NĐ-CP | *Hà Nội, ngày 19 tháng 8 năm 2026* |

# 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
## QUY ĐỊNH CHUNG

### Điều 1. Phạm vi điều chỉnh

1. 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 gồm các nội dung sau đây:

a) Nội dung, trình tự, thủ tục, thẩm quyền áp dụng 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; đấu tranh bảo vệ 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, tin giả 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 theo quy định của pháp luật;

b) Bảo đảm an ninh thông tin mạng theo quy định tại khoản 2 và khoản 3 Điều 25 Luật An ninh mạng;

c) Chuẩn kiến thức, kỹ năng chuyên sâu về an ninh mạng; chương trình, nội dung việc chứng nhận tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng.

2. Nghị định này quy định các biện pháp thi hành 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 và nguyên tắc áp dụng**

1. 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.

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

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

4. 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.

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

6. Hành vi vi phạm pháp luật về an ninh thông tin mạng là hành vi vi phạm pháp luật về an ninh mạng phát sinh trong hoạt động bảo đảm an ninh thông tin mạng, được thực hiện thông qua không gian mạng, hệ thống thông tin, công nghệ thông tin, phương tiện điện tử hoặc thiết bị số, thuộc trường hợp quy định tại Điều 7 hoặc Điều 13 của Luật An ninh mạng.

7. 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.

8. 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. 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 được thực hiện đối với thiết kế, đề án, kế hoạch, phương án xây dựng mới, nâng cấp, mở rộng hệ thống thông tin quan trọng về an ninh quốc gia trước khi phê duyệt, nhằm xem xét, đánh giá việc đáp ứng yêu cầu về an ninh mạng của hệ thống thông tin.

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

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

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

a) Việc tuân thủ quy định, tiêu chuẩn, quy chuẩn, điều kiện về an ninh mạng trong thiết kế, xây dựng, nâng cấp, mở rộng hệ thống thông tin;

b) Sự phù hợp của phương án bảo vệ an ninh mạng, phương án ứng phó, khắc phục sự cố an ninh mạng;

c) Việc bố trí nhân lực, điều kiện kỹ thuật, biện pháp quản lý để bảo vệ an ninh mạng đối với hệ thống thông tin;

d) Nội dung khác có liên quan trực tiếp đến yêu cầu bảo vệ an ninh mạng đối với hệ thống thông tin được thẩm định.

5. Thẩm quyền thẩm định an ninh mạng được quy định như sau:

a) Bộ Công an 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 Quốc phòng 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.

6. Hồ sơ đề nghị thẩm định an ninh mạng gồm:

a) Văn bản đề nghị thẩm định an ninh mạng theo Mẫu số 01 Phụ lục ban hành kèm theo Nghị định này;

b) Hồ sơ, tài liệu về đối tượng thẩm định an ninh mạng, gồm: hồ sơ thiết kế chi tiết dự án đầu tư xây dựng mới, nâng cấp, mở rộng hệ thống thông tin; đề án, kế hoạch, phương án nâng cấp, mở rộng hệ thống thông tin;

c) Tài liệu thể hiện kết quả xác định cấp độ an ninh mạng của hệ thống thông tin;

d) Tài liệu khác có liên quan đến nội dung đề nghị thẩm định, nếu có.

7. Trình tự, thủ tục thẩm định an ninh mạng được thực hiện như sau:

a) Sau khi hệ thống thông tin được xác định cấp độ hệ thống thông tin theo quy định của pháp luật, chủ quản hệ thống thông tin gửi 01 bộ hồ sơ đề nghị thẩm định an ninh mạng đến cơ quan có thẩm quyền quy định tại khoản 5 Điều này;

b) Trong thời hạn 03 ngày làm việc kể từ ngày nhận được hồ sơ, cơ quan có thẩm quyền có trách nhiệm kiểm tra tính hợp lệ của hồ sơ. Trường hợp hồ sơ hợp lệ thì cấp giấy tiếp nhận hồ sơ ngay sau khi hoàn thành việc kiểm tra. Trường hợp hồ sơ chưa hợp lệ thì thông báo bằng văn bản để chủ quản hệ thống thông tin bổ sung, hoàn thiện hồ sơ;

c) Trong thời hạn tối đa 25 ngày làm việc kể từ ngày cấp giấy tiếp nhận hồ sơ hợp lệ, cơ quan có thẩm quyền tổ chức thẩm định an ninh mạng và thông báo kết quả thẩm định bằng văn bản cho chủ quản hệ thống thông tin.

8. Trường hợp cần xác định sự phù hợp giữa hiện trạng hệ thống thông tin với hồ sơ đề nghị thẩm định, cơ quan có thẩm quyền tiến hành khảo sát, đánh giá thực tế hệ thống thông tin. Việc khảo sát, đánh giá thực tế không được làm ảnh hưởng đến hoạt động bình thường của chủ quản hệ thống thông tin và hệ thống

thông tin được thẩm định. Thời gian khảo sát, đánh giá thực tế không quá 07 ngày làm việc và không tính vào thời hạn thẩm định quy định tại điểm c khoản 7 Điều này.

9. Kết quả thẩm định an ninh mạng là căn cứ để chủ quản hệ thống thông tin hoàn thiện phương án bảo đảm an ninh mạng, trình cấp có thẩm quyền phê duyệt hoặc thực hiện các bước tiếp theo theo quy định của pháp luật.

10. Hồ sơ, tài liệu, thông tin và kết quả thẩm định an ninh mạng được quản lý, bảo vệ theo quy định của pháp luật về bảo vệ bí mật nhà nước, an ninh mạng và quy định khác của pháp luật có liên quan.

**Điều 6. 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 là thủ tục do cơ quan có thẩm quyền thực hiện để xem xét, xác định mức độ đáp ứng điều kiện an ninh mạng của hệ thống thông tin quan trọng về an ninh quốc gia trước khi đưa vào vận hành, sử dụng.

2. Hệ thống thông tin quan trọng về an ninh quốc gia phải được đánh giá, chứng nhận đủ điều kiện an ninh mạng trước khi đưa vào vận hành, sử dụng; chủ quản hệ thống thông tin có trách nhiệm duy trì việc đáp ứng điều kiện an ninh mạng trong suốt quá trình quản lý, vận hành, khai thác hệ thống.

3. Hệ thống thông tin quan trọng về an ninh quốc gia được đánh giá đủ điều kiện an ninh mạng khi đáp ứng các yêu cầu sau đây:

a) Có quy định, quy trình, phương án bảo đảm an ninh mạng phù hợp với quy định của pháp luật về an ninh mạng, bảo vệ bí mật nhà nước, tiêu chuẩn, quy chuẩn kỹ thuật về an ninh mạng và tiêu chuẩn kỹ thuật chuyên ngành có liên quan;

b) Xác định rõ hệ thống thông tin, thông tin, dữ liệu, hạ tầng kỹ thuật và thành phần quan trọng cần ưu tiên bảo vệ; quy trình quản lý, vận hành, khai thác, sử dụng, bảo vệ hệ thống thông tin, dữ liệu, hạ tầng kỹ thuật; trách nhiệm của từng bộ phận, cá nhân trong quản lý, vận hành, sử dụng hệ thống;

c) Có bộ phận hoặc nhân sự phụ trách vận hành, quản trị hệ thống và bảo vệ an ninh mạng; nhân sự thực hiện nhiệm vụ này có trình độ chuyên môn phù hợp về an ninh mạng, công nghệ thông tin hoặc lĩnh vực kỹ thuật có liên quan và có trách nhiệm bảo mật thông tin liên quan đến hệ thống thông tin trong thời gian thực hiện nhiệm vụ và sau khi chấm dứt nhiệm vụ;

d) Hoạt động vận hành, quản trị hệ thống và bảo vệ an ninh mạng được phân định rõ chức năng, nhiệm vụ, quyền hạn, trách nhiệm; bảo đảm kiểm soát chéo, hạn chế xung đột nhiệm vụ và đáp ứng yêu cầu bảo vệ an ninh mạng;

đ) Thiết bị, phần cứng, phần mềm, cơ sở dữ liệu, mã nguồn, chương trình ứng dụng, công cụ phát triển và thành phần kỹ thuật khác của hệ thống được kiểm tra, quản lý, rà soát, cập nhật, khắc phục điểm yếu, lỗ hổng bảo mật, mã độc, phần cứng độc hại và nguy cơ mất an ninh mạng trước khi đưa vào sử dụng và trong quá trình vận hành;

e) Sản phẩm, thiết bị, phần cứng, phần mềm 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 chỉ được đưa vào sử dụng sau khi đã có biện pháp xử lý, khắc phục nguy cơ gây mất an ninh mạng;

g) Có biện pháp quản lý, kiểm tra, kiểm soát việc kết nối, sử dụng, vận chuyển, lưu trữ, sửa chữa, tiêu hủy thiết bị công nghệ thông tin, phương tiện truyền thông, vật mang tin, thiết bị di động, thiết bị và phương tiện lưu trữ thông tin phục vụ hoạt động của hệ thống thông tin;

h) Có biện pháp kỹ thuật để giám sát, phát hiện, cảnh báo, ngăn chặn, xử lý nguy cơ, sự cố an ninh mạng; tách biệt môi trường vận hành chính thức với môi trường phát triển, kiểm tra, thử nghiệm; kiểm soát việc cài đặt, sử dụng phần mềm, dịch vụ, công cụ, phương tiện trên hệ thống;

i) Có phương án sao lưu dự phòng dữ liệu, kiểm tra khả năng khôi phục dữ liệu; phân vùng mạng theo đối tượng sử dụng, mục đích sử dụng, mức độ quan trọng của tài nguyên hệ thống; kiểm soát kết nối, kiểm soát truy cập giữa các vùng mạng và tài nguyên quan trọng của hệ thống;

k) Có giải pháp phát hiện, ngăn chặn truy cập không tin cậy, xâm nhập trái phép, tấn công từ chối dịch vụ và hình thức tấn công mạng khác; dò tìm, phát hiện, cảnh báo và xử lý điểm yếu, lỗ hổng kỹ thuật, kết nối, thiết bị, phần mềm cài đặt trái phép vào hệ thống;

l) Ghi, quản lý, lưu trữ nhật ký hoạt động của hệ thống thông tin, người sử dụng, lỗi phát sinh và sự cố an ninh mạng theo quy định của pháp luật, tiêu chuẩn, quy chuẩn kỹ thuật có liên quan và yêu cầu bảo vệ an ninh mạng;

m) Có biện pháp quản lý tài khoản, phân quyền sử dụng, kiểm soát truy cập, quản lý mã khóa bí mật, phương thức xác thực; kiểm soát việc tạo lập, cấp phát, sử dụng, giám sát tài khoản có quyền quản trị; rà soát, kiểm tra, xét duyệt lại quyền truy cập của người sử dụng;

n) Có biện pháp bảo đảm an ninh vật lý đối với địa điểm lắp đặt hệ thống, trung tâm dữ liệu, khu vực đặt máy chủ, thiết bị mạng, thiết bị lưu trữ và khu vực kỹ thuật trọng yếu; bảo đảm nguồn điện, hệ thống hỗ trợ vận hành liên tục, kiểm soát ra vào và phòng ngừa nguy cơ xâm nhập, thu thập thông tin trái phép bằng thiết bị, phương tiện kỹ thuật;

o) Việc xử lý, lưu trữ, truyền đưa thông tin thuộc bí mật nhà nước trên hệ thống thông tin phải tuân thủ quy định của pháp luật về bảo vệ bí mật nhà nước, pháp luật về cơ yếu, pháp luật về an ninh mạng và quy định khác của pháp luật có liên quan; hệ thống thông tin xử lý bí mật nhà nước phải được áp dụng biện pháp bảo vệ phù hợp với cấp độ bí mật và yêu cầu bảo vệ an ninh mạng.

4. Nội dung đánh giá điều kiện an ninh mạng bao gồm việc xem xét, xác định mức độ đáp ứng các điều kiện quy định tại khoản 3 Điều này và các yêu cầu khác có liên quan trực tiếp đến việc bảo đảm an ninh mạng đối với hệ thống thông tin được đánh giá.

5. Thẩm quyền đánh giá, chứng nhận đủ điều kiện an ninh mạng được quy định như sau:

a) Bộ Công an 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 Quốc phòng đánh giá, chứng nhận đủ điều kiện an ninh mạng đối với hệ thống thông tin quân sự;

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

6. Hồ sơ đề nghị đánh giá điều kiện an ninh mạng gồm:

a) Văn bản đề nghị chứng nhận đủ điều kiện an ninh mạng theo Mẫu số 02 Phụ lục ban hành kèm theo Nghị định này;

b) Báo cáo nghiên cứu khả thi, hồ sơ thiết kế kỹ thuật, hồ sơ thiết kế thi công hoặc tài liệu tương đương của dự án đầu tư xây dựng, nâng cấp, mở rộng hệ thống thông tin;

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

d) Tài liệu thể hiện kết quả thẩm định an ninh mạng, nếu có;

đ) Tài liệu khác có liên quan đến nội dung đề nghị đánh giá, nếu có.

7. Trình tự, thủ tục đánh giá điều kiện an ninh mạng được thực hiện như sau:

a) Chủ quản hệ thống thông tin gửi 01 bộ hồ sơ đề nghị đánh giá điều kiện an ninh mạng đến cơ quan có thẩm quyền quy định tại khoản 5 Điều này;

b) Trong thời hạn tối đa 03 ngày làm việc kể từ ngày nhận được hồ sơ, cơ quan có thẩm quyền có trách nhiệm kiểm tra tính hợp lệ của hồ sơ. Trường hợp hồ sơ hợp lệ thì cấp giấy tiếp nhận hồ sơ ngay sau khi hoàn thành việc kiểm tra. Trường hợp hồ sơ chưa hợp lệ thì thông báo bằng văn bản để chủ quản hệ thống thông tin bổ sung, hoàn thiện hồ sơ;

c) Trong thời hạn tối đa 25 ngày làm việc kể từ ngày cấp giấy tiếp nhận hồ sơ hợp lệ, cơ quan có thẩm quyền tổ chức đánh giá điều kiện an ninh mạng;

d) Trường hợp hệ thống thông tin đáp ứng đủ điều kiện an ninh mạng, Thủ trưởng cơ quan có thẩm quyền cấp Giấy chứng nhận đủ điều kiện an ninh mạng đối với hệ thống thông tin;

đ) Trường hợp hệ thống thông tin chưa đáp ứng điều kiện an ninh mạng, cơ quan có thẩm quyền thông báo bằng văn bản, nêu rõ nội dung chưa đáp ứng và yêu cầu chủ quản hệ thống thông tin bổ sung, hoàn thiện, nâng cấp, khắc phục trước khi đưa hệ thống thông tin vào vận hành, sử dụng.

8. Chủ quản hệ thống thông tin có trách nhiệm bổ sung, hoàn thiện, nâng cấp, khắc phục các nội dung chưa đáp ứng theo yêu cầu của cơ quan có thẩm quyền quy định tại điểm đ khoản 7 Điều này và bảo đảm hệ thống thông tin đáp ứng điều kiện an ninh mạng trước khi đưa vào vận hành, sử dụng.

9. Việc duy trì điều kiện an ninh mạng của hệ thống thông tin được kiểm tra, hậu kiểm theo quy định của pháp luật. Trường hợp chủ quản hệ thống thông tin không thực hiện hoặc thực hiện không đầy đủ yêu cầu quy định tại khoản 8 Điều này mà đưa hệ thống thông tin vào vận hành, sử dụng thì bị xử lý theo quy định của pháp luật.

10. Giấy chứng nhận đủ điều kiện an ninh mạng là căn cứ để chủ quản hệ thống thông tin đưa hệ thống thông tin quan trọng về an ninh quốc gia vào vận hành, sử dụng theo quy định của pháp luật.

11. Hồ sơ, tài liệu, thông tin và kết quả đánh giá điều kiện an ninh mạng được quản lý, bảo vệ theo quy định của pháp luật về bảo vệ bí mật nhà nước, an ninh mạng và quy định khác của pháp luật có liên quan.

**Điều 7. Trình tự, thủ tục giám sát an ninh mạng**

1. Giám sát an ninh mạng là hoạt động thu thập, tiếp nhận, phân tích, xử lý thông tin nhằm phát hiện, cảnh báo 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, ngăn chặn, xử lý và khắc phục.

2. Chủ quản hệ thống thông tin có trách nhiệm tổ chức giám sát an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý; xây dựng cơ chế tự giám sát, tự cảnh báo, tiếp nhận cảnh báo về nguy cơ đe dọa an ninh mạng, sự cố an ninh mạng, điểm yếu, lỗ hổng bảo mật; duy trì hệ thống giám sát an ninh

mạng, hệ thống phòng, chống mã độc tập trung đáp ứng yêu cầu kết nối, chia sẻ dữ liệu cảnh báo nguy cơ, sự cố an ninh mạng với cơ quan có thẩm quyền theo quy định của pháp luật.

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; bảo đảm điều kiện kỹ thuật, nhân lực và thông tin cần thiết phục vụ hoạt động 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 các đối tượng sau đây, trừ hệ thống thông tin quân sự và hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ:

a) Không gian mạng quốc gia;

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 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. Trình tự thực hiện giám sát an ninh mạng của lực lượng chuyên trách bảo vệ an ninh mạng được quy định như sau:

a) Trước khi triển khai biện pháp giám sát an ninh mạng, lực lượng chuyên trách bảo vệ an ninh mạng thông báo bằng văn bản cho chủ quản hệ thống thông tin về lý do, phạm vi, nội dung, thời gian và yêu cầu phối hợp giám sát, trừ trường hợp khẩn cấp nhằm bảo vệ an ninh quốc gia;

b) Trường hợp khẩn cấp không thể thông báo trước, lực lượng chuyên trách bảo vệ an ninh mạng triển khai ngay biện pháp giám sát an ninh mạng và gửi văn bản thông báo cho chủ quản hệ thống thông tin trong thời hạn 24 giờ kể từ thời điểm triển khai;

c) Lực lượng chuyên trách bảo vệ an ninh mạng triển khai biện pháp kỹ thuật giám sát an ninh mạng theo phạm vi, nội dung đã thông báo hoặc theo yêu cầu xử lý tình huống khẩn cấp;

d) Thông tin thu thập được trong quá trình giám sát phải được phân tích, đánh giá để kịp thời phát hiện, cảnh báo nguy cơ đe dọa an ninh mạng, sự cố an ninh mạng, điểm yếu, lỗ hổng bảo mật, mã độc, phần cứng độc hại;

đ) Trường hợp phát hiện nguy cơ, sự cố an ninh mạng hoặc dấu hiệu ảnh hưởng đến an ninh quốc gia, trật tự, an toàn xã hội, lực lượng chuyên trách bảo vệ an ninh mạng thông báo kịp thời cho chủ quản hệ thống thông tin để phối hợp xử lý, khắc phục;

e) Kết quả giám sát an ninh mạng được tổng hợp, thông báo cho chủ quản hệ thống thông tin trong phạm vi cần thiết và báo cáo cơ quan có thẩm quyền theo quy định của pháp luật.

6. Trong quá trình giám sát an ninh mạng, chủ quản hệ thống thông tin có trách nhiệm:

a) Phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng trong việc triển khai biện pháp 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 của lực lượng chuyên trách bảo vệ an ninh mạng;

c) Cung cấp, cập nhật thông tin liên quan đến cấu hình, kết nối, vận hành hệ thống thông tin khi có yêu cầu của cơ quan có thẩm quyền;

d) Tiếp nhận, xử lý cảnh báo nguy cơ, sự cố an ninh mạng và thực hiện biện pháp khắc phục theo yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng.

7. Doanh nghiệp viễn thông, doanh nghiệp cung cấp dịch vụ Internet, công nghệ thông tin có trách nhiệm phối hợp, cung cấp thông tin, dữ liệu kỹ thuật cần thiết và hỗ trợ lực lượng chuyên trách bảo vệ an ninh mạng trong hoạt động giám sát an ninh mạng theo quy định của pháp luật.

8. Việc giám sát an ninh mạng phải bảo đảm đúng thẩm quyền, phạm vi, mục đích, yêu cầu bảo vệ an ninh mạng; không làm ảnh hưởng trái pháp luật đến hoạt động bình thường của cơ quan, tổ chức, cá nhân và hệ thống thông tin được giám sát.

9. Thông tin, tài liệu, dữ liệu thu thập được từ hoạt động giám sát an ninh mạng được quản lý, sử dụng, bảo vệ theo quy định của pháp luật về bảo vệ bí mật nhà nước, an ninh mạng và quy định khác của pháp luật có liên quan.

**Điều 8. Trình tự, thủ tục 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, 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, sự cố 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 làm ảnh hưởng đến yêu cầu bảo đảm an ninh mạng;

c) Kiểm tra định kỳ hằng năm;

d) Kiểm tra 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; 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. Đối tượng kiểm tra an ninh mạng bao gồm:

a) Hệ thống phần cứng, phần mềm, thiết bị số, thiết bị mạng và thành phần kỹ thuật khác của hệ thống thông tin;

b) Quy định, quy trình, phương án, 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, kế hoạch ứng phó, khắc phục sự cố an ninh mạng;

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

e) Nhân lực tham gia quản trị, vận hành, bảo vệ an ninh mạng đối với hệ thống thông tin.

4. Nội dung kiểm tra an ninh mạng bao gồm:

a) Việc tuân thủ 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 quy định, quy trình, phương án, biện pháp bảo đảm an ninh mạng;

c) Việc triển khai, duy trì và hiệu quả của phương án, kế hoạch ứng phó, khắc phục sự cố an ninh mạng;

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

đ) Nội dung khác phù hợp với mục đích kiểm tra, tính chất, yêu cầu bảo vệ an ninh mạng của hệ thống thông tin.

5. 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) Gửi văn bản thông báo kết quả kiểm tra an ninh mạng định kỳ hằng năm cho lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền trước ngày 01 tháng 10 hằng năm;

c) Phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng trong quá trình kiểm tra an ninh mạng đột xuất;

d) Thực hiện yêu cầu khắc phục nguy cơ, sự cố an ninh mạng, điểm yếu, lỗ hổng bảo mật theo kết luận kiểm tra của cơ quan có thẩm quyền.

6. Kiểm tra an ninh mạng đột xuất đối với hệ thống thông tin quan trọng về an ninh quốc gia được quy định như sau:

a) Trước thời điểm tiến hành kiểm tra, lực lượng chuyên trách bảo vệ an ninh mạng có trách nhiệm thông báo bằng văn bản cho chủ quản hệ thống thông tin ít nhất là 12 giờ trong trường hợp xảy ra sự cố an ninh mạng, hành vi xâm phạm an ninh mạng; ít nhất là 72 giờ trong trường hợp có yêu cầu quản lý nhà nước về an ninh mạng hoặc hết thời hạn khắc phục điểm yếu, lỗ hổng bảo mật theo khuyến cáo của lực lượng chuyên trách bảo vệ an ninh mạng;

b) Trong thời hạn 25 ngày làm việc kể từ ngày kết thúc kiểm tra, lực lượng chuyên trách bảo vệ an ninh mạng thông báo kết quả kiểm tra và đưa ra yêu cầu đối với chủ quản hệ thống thông tin trong trường hợp 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;

c) Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an kiểm tra an ninh mạng đột xuất đối với hệ thống thông tin quan trọng về an ninh quốc gia, trừ hệ thống thông tin quân sự do Bộ Quốc phòng quản lý, hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ và sản phẩm mật mã do Ban Cơ yếu Chính phủ cung cấp để bảo vệ thông tin thuộc bí mật nhà nước.

Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng kiểm tra an ninh mạng đột xuất đối với hệ thống thông tin quân sự.

Ban Cơ yếu Chính phủ kiểm tra an ninh mạng đột xuất đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ và sản phẩm mật mã do Ban Cơ yếu Chính phủ cung cấp để bảo vệ thông tin thuộc bí mật nhà nước;

d) Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng tiến hành kiểm tra an ninh mạng đột xuất.

7. Trình tự, thủ tục kiểm tra an ninh mạng do lực lượng chuyên trách bảo vệ an ninh mạng thực hiện được quy định như sau:

a) Thông báo kế hoạch kiểm tra hoặc quyết định kiểm tra an ninh mạng cho chủ quản hệ thống thông tin, trừ trường hợp kiểm tra đột xuất nhằm kịp thời ngăn chặn nguy cơ xâm hại an ninh quốc gia, trật tự, an toàn xã hội;

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

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

d) Lập biên bản về quá trình, nội dung và kết quả kiểm tra an ninh mạng;

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

e) Yêu cầu chủ quản hệ thống thông tin khắc phục nguy cơ, sự cố an ninh mạng, điểm yếu, lỗ hổng bảo mật hoặc vi phạm pháp luật về an ninh mạng được phát hiện qua kiểm tra, nếu có.

8. Trường hợp kiểm tra đột xuất mà không thể thông báo trước, lực lượng chuyên trách bảo vệ an ninh mạng triển khai ngay việc kiểm tra theo thẩm quyền và thông báo bằng văn bản cho chủ quản hệ thống thông tin trong thời hạn 24 giờ kể từ thời điểm bắt đầu kiểm tra.

9. Trường hợp cần giữ nguyên hiện trạng hệ thống thông tin để phục vụ điều tra, xác minh, xử lý vi phạm pháp luật, xử lý 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 thực hiện một hoặc một số biện pháp cần thiết, bao gồm tạm thời giữ nguyên cấu hình, trạng thái kỹ thuật, dữ liệu, nhật ký hệ thống; hạn chế, điều chỉnh hoặc tạm ngừng một phần hoạt động của hệ thống thông tin. Văn bản yêu cầu phải nêu rõ lý do, mục đích, phạm vi, biện pháp áp dụng và thời hạn thực hiện.

10. Việc kiểm tra an ninh mạng phải bảo đảm đúng thẩm quyền, căn cứ, mục đích, phạm vi, nội dung kiểm tra; không làm ảnh hưởng trái pháp luật đến hoạt động bình thường của cơ quan, tổ chức, cá nhân và hệ thống thông tin được kiểm tra.

11. Biên bản kiểm tra, kết quả kiểm tra, thông tin, tài liệu, dữ liệu thu thập được trong quá trình kiểm tra an ninh mạng được quản lý, sử dụng, bảo vệ theo quy định của pháp luật về bảo vệ bí mật nhà nước, an ninh mạng và quy định khác của pháp luật có liên quan.

**Điều 9. 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. Ứng phó, khắc phục sự cố an ninh mạng là hoạt động phát hiện, xác định, ngăn chặn, hạn chế, xử lý, khắc phục và khôi phục hoạt động của 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, bảo quản thông tin, dữ liệu, tài liệu, chứng cứ liên quan đến sự cố an ninh mạng;

c) Khoanh vùng, cô lập, hạn chế phạm vi ảnh hưởng của sự cố an ninh mạng;

d) Phân tích, đánh giá, phân loại, xác định mức độ sự cố an ninh mạng;

đ) Triển khai biện pháp ứng phó, khắc phục, khôi phục hoạt động bình thường của hệ thống thông tin;

e) Xác minh nguyên nhân, truy tìm nguồn gốc sự cố an ninh mạng.

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

a) Xây dựng, ban hành, tổ chức thực hiện và 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 phát hiện, xác định, phân loại sự cố an ninh mạng và triển khai phương án ứng phó, khắc phục sự cố an ninh mạng;

c) Thông báo ngay cho lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền khi sự cố an ninh mạng vượt quá khả năng xử lý hoặc xuất hiện tình huống nguy hiểm về an ninh mạng;

d) Phối hợp, cung cấp thông tin, tài liệu, dữ liệu, điều kiện kỹ thuật cần thiết để lực lượng chuyên trách bảo vệ an ninh mạng thực hiện nhiệm vụ điều phối, ứng phó, khắc phục sự cố an ninh mạng;

đ) Báo cáo kết quả xử lý, khắc phục sự cố an ninh mạng với lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền theo quy định.

4. Việc thông báo, báo cáo sự cố an ninh mạng quy định tại điểm c và điểm đ khoản 3 Điều này không áp dụng đối với hệ thống thông tin quân sự và hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ. Việc thông báo, báo cáo sự cố an ninh mạng đối với hệ thống thông tin quân sự và hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ thực hiện theo quy định của Bộ Quốc phòng và pháp luật về cơ yếu.

5. Khi tiếp nhận thông tin về sự cố an ninh mạng, lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền thực hiện các nhiệm vụ sau đây:

a) Hướng dẫn chủ quản hệ thống thông tin áp dụng biện pháp tạm thời để ngăn chặn, hạn chế thiệt hại;

b) Đánh giá tính chất, mức độ, phạm vi ảnh hưởng của sự cố an ninh mạng;

c) Quyết định hoặc đề xuất phương án điều phối, ứng phó, khắc phục sự cố an ninh mạng theo thẩm quyền;

d) Điều hành, giám sát hoạt động ứng phó, khắc phục sự cố an ninh mạng trong trường hợp cần thiết;

đ) Tổng hợp, báo cáo, đánh giá kết quả xử lý sự cố an ninh mạng theo quy định.

6. Trường hợp khẩn cấp nhằm bảo vệ an ninh quốc gia, trật tự, an toàn xã hội, lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền được áp dụng ngay biện pháp điều phối, ứng phó, khắc phục sự cố an ninh mạng cần thiết theo quy định của pháp luật; đồng thời thông báo cho chủ quản hệ thống thông tin để phối hợp thực hiện.

7. Trình tự điều phối, ứng phó, khắc phục sự cố an ninh mạng được thực hiện như sau:

a) Chủ quản hệ thống thông tin phát hiện, xác định, phân loại sự cố an ninh mạng và triển khai ngay biện pháp ứng phó ban đầu;

b) Trường hợp sự cố vượt quá khả năng xử lý hoặc xuất hiện tình huống nguy hiểm về an ninh mạng, chủ quản hệ thống thông tin thông báo cho lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền;

c) Lực lượng chuyên trách bảo vệ an ninh mạng đánh giá sự cố, hướng dẫn hoặc quyết định phương án điều phối, ứng phó, khắc phục sự cố an ninh mạng theo thẩm quyền;

d) Chủ quản hệ thống thông tin thực hiện biện pháp ứng phó, khắc phục sự cố an ninh mạng theo phương án đã được xác định hoặc theo hướng dẫn của lực lượng chuyên trách bảo vệ an ninh mạng;

đ) Cơ quan, tổ chức, doanh nghiệp, cá nhân có liên quan phối hợp, cung cấp thông tin, hỗ trợ kỹ thuật, nguồn lực cần thiết phục vụ hoạt động điều phối, ứng phó, khắc phục sự cố an ninh mạng theo yêu cầu của cơ quan có thẩm quyền;

e) Sau khi hoàn thành việc ứng phó, khắc phục sự cố, chủ quản hệ thống thông tin tổng hợp kết quả xử lý, đánh giá nguyên nhân, hậu quả, biện pháp đã áp dụng và gửi báo cáo cho lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền.

8. 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, 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, bộ, ngành, địa phương, cơ quan, tổ chức, doanh nghiệp, cá nhân có liên quan theo quy định của pháp luật.

9. Doanh nghiệp viễn thông, doanh nghiệp cung cấp dịch vụ Internet, doanh nghiệp công nghệ thông tin có trách nhiệm phối hợp, cung cấp thông tin, dữ liệu kỹ thuật, bố trí điều kiện kỹ thuật cần thiết để lực lượng chuyên trách bảo vệ an ninh mạng thực hiện nhiệm vụ điều phối, ứng phó, khắc phục sự cố an ninh mạng theo quy định của pháp luật.

10. Thông tin, tài liệu, dữ liệu, chứng cứ thu thập được trong quá trình ứng phó, khắc phục sự cố an ninh mạng được quản lý, sử dụng, bảo vệ theo quy định của pháp luật về bảo vệ bí mật nhà nước, an ninh mạng và quy định khác của pháp luật có liên quan.

**Điều 10. 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 11. Trình tự, thủ tục thực hiện biện pháp yêu cầu xóa bỏ thông tin trái pháp luật hoặc thông tin sai sự thật, tin giả 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. Lực lượng chuyên trách bảo vệ an ninh mạng 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, tin giả 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, tin giả 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 theo chức năng, nhiệm vụ, quyền hạn được giao quyết định áp dụng biện pháp yêu cầu xóa bỏ thông tin trái pháp luật hoặc thông tin sai sự thật, tin giả 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 12. 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) Lực lượng chuyên trách bảo vệ an ninh mạng 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) 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 của pháp luật, bảo đảm 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 13. 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. Lực lượng chuyên trách bảo vệ an ninh mạng 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 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, 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, 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 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 14. 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, kinh tế, 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 15. 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 16. 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 phát triển tiếp (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 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 pháp luật về 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 thông tin, dịch vụ, ứng dụng vi phạm pháp luật về an ninh thông tin mạng theo yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an;

b) Việc thực hiện yêu cầu quy định tại điểm a khoản này phải hoàn thành chậm nhất trong thời hạn 24 giờ kể từ thời điểm nhận được yêu cầu; trường hợp khẩn cấp đe dọa xâm hại an ninh quốc gia thì phải hoàn thành chậm nhất trong thời hạn 06 giờ kể từ thời điểm nhận được yêu cầu;

c) Áp dụng biện pháp quản lý nhà nước, biện pháp kỹ thuật để 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) Hạn chế hiển thị tại Việt Nam hoặc khóa tạm thời tài khoản cá nhân, trang, nhóm cộng đồng, kênh nội dung được sử dụng để đăng tải thông tin vi phạm pháp luật về an ninh thông tin mạng trong các trường hợp sau đây:

Trong thời hạn 30 ngày, đăng tải từ 03 lần trở lên thông tin vi phạm pháp luật về an ninh thông tin mạng thì bị hạn chế hiển thị tại Việt Nam hoặc khóa tạm thời với thời hạn tối đa 60 ngày, căn cứ tính chất, mức độ vi phạm;

Trong thời hạn 90 ngày, đăng tải từ 10 lần trở lên thông tin vi phạm pháp luật về an ninh thông tin mạng thì bị hạn chế hiển thị tại Việt Nam hoặc khóa tạm thời với thời hạn tối đa 180 ngày, căn cứ tính chất, mức độ vi phạm.

đ) Hạn chế hiển thị vô thời hạn tại Việt Nam hoặc khóa tài khoản vô thời hạn đối với tài khoản cá nhân, trang, nhóm cộng đồng, kênh nội dung được sử dụng để thực hiện, tiếp tục thực hiện, phát tán, tổ chức, điều hành hoặc hỗ trợ thực hiện hành vi vi phạm pháp luật về an ninh mạng trong các trường hợp sau đây:

Đăng tải, phát tán thông tin 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 tiếp tục được sử dụng để thực hiện hành vi vi phạm pháp luật về an ninh mạng;

Có căn cứ xác định tài khoản cá nhân, trang, nhóm cộng đồng, kênh nội dung tiếp tục được sử dụng làm công cụ, phương tiện thực hiện hành vi vi phạm pháp luật về an ninh mạng và việc áp dụng biện pháp khóa tài khoản vô thời hạn là cần thiết, phù hợp với tính chất, mức độ vi phạm.

e) Tài khoản bị áp dụng biện pháp khóa tài khoản vô thời hạn được xem xét khôi phục trong các trường hợp sau đây: không còn căn cứ áp dụng biện pháp; có nhầm lẫn trong quá trình xác minh, xử lý; xuất hiện tình tiết mới làm thay đổi căn cứ áp dụng biện pháp; cơ quan có thẩm quyền xác định tài khoản không được sử dụng để thực hiện hành vi vi phạm pháp luật về an ninh mạng.

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, cổng nguồn khi 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, đáp ứng yêu cầu xác minh, điều tra, xử lý hành vi vi phạm pháp luật.

**Điều 17. 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 15 của Nghị định này và không xâm phạm trái pháp luật quyền, lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

**Điều 18. Trách nhiệm 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. Doanh nghiệp viễn thông, doanh nghiệp cung cấp dịch vụ Internet, dịch vụ lưu trữ web (hosting), dịch vụ trung tâm dữ liệu (data center) và các doanh nghiệp cung cấp dịch vụ ứng dụng viễn thông có trách nhiệm:

a) Thực hiện ngăn chặn, gỡ bỏ các nội dung, dịch vụ, ứng dụng trên mạng vi phạm pháp luật chậm nhất là 24 giờ kể từ khi có yêu cầu bằng văn bản, điện thoại hoặc thư điện tử của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an;

b) Từ chối cung cấp hoặc tạm ngừng cung cấp dịch vụ viễn thông, dịch vụ Internet, các dịch vụ khác đối với tổ chức, cá nhân sử dụng dịch vụ để đăng tải thông tin vi phạm pháp luật trên mạng theo yêu cầu hợp lệ của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an;

c) Doanh nghiệp viễn thông, doanh nghiệp cung cấp dịch vụ Internet kết nối, nhận yêu cầu điều phối ngăn chặn, gỡ bỏ thông tin xấu độc, vi phạm pháp luật, báo cáo kết quả qua hệ thống kỹ thuật và thực hiện các biện pháp xử lý khác theo yêu cầu của Bộ Công an;

d) Doanh nghiệp viễn thông, doanh nghiệp cung cấp dịch vụ Internet có trách nhiệm bảo đảm hạ tầng kỹ thuật, hệ thống kết nối, năng lực xử lý, truyền tải, chia sẻ thông tin, dữ liệu và các điều kiện cần thiết khác trong quá trình cung cấp dịch vụ để đáp ứng yêu cầu bảo đảm an ninh thông tin mạng, phục vụ triển khai các giải pháp, biện pháp bảo vệ an ninh mạng theo quy định của pháp luật và yêu cầu hợp lệ của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an.

3. 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 19. 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) 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.

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 lực lượng chuyên trách bảo vệ an ninh mạng 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 lực lượng chuyên trách bảo vệ an ninh mạng 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 25 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 lực lượng chuyên trách bảo vệ an ninh mạng 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 lực lượng chuyên trách bảo vệ an ninh mạng 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) Lực lượng chuyên trách bảo vệ an ninh mạng 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 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 20. 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 19 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 19 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 21. 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 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, quản lý thông tin phục vụ định danh địa chỉ IP gắn với thông tin thuê bao, thời điểm sử dụng dịch vụ và thông tin về 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 22. 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 23. 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 định danh cá nhân, 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 24. Yêu cầu về kiến thức, kỹ năng chuyên sâu về an ninh mạng

1. Các đối tượng quy định tại khoản 1 Điều 34 của Luật An ninh mạng được xác định đáp ứng yêu cầu về kiến thức, kỹ năng chuyên sâu về an ninh mạng khi đáp ứng một trong các tiêu chí sau:

a) Đã được đào tạo từ đại học trở lên chuyên ngành an ninh mạng;

b) Đã được đào tạo từ đại học trở lên các ngành về công nghệ thông tin hoặc ngành gần đào tạo về công nghệ thông tin và có chứng chỉ chuyên môn về an ninh mạng quy định tại khoản 5 Điều này;

c) Đã được đào tạo từ đại học trở lên các ngành về công nghệ thông tin hoặc ngành gần đào tạo về công nghệ thông tin và có tối thiểu 5 năm kinh nghiệm công tác bảo vệ an ninh mạng và phòng chống tội phạm sử dụng công nghệ cao;

d) Đã được đào tạo từ đại học trở lên các ngành về công nghệ thông tin hoặc ngành gần đào tạo về công nghệ thông tin và được tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng quy định tại khoản 2 Điều này.

2. Căn cứ vào vị trí việc làm, chức năng, nhiệm vụ được giao, các đối tượng quy định tại khoản 2 Điều 34 của Luật An ninh mạng phải được tập huấn kiến thức, kỹ năng nền tảng về an ninh mạng quy định tại khoản 3 Điều này và ít nhất một kiến thức, kỹ năng chuyên sâu về an ninh mạng quy định tại khoản 4 Điều này, trừ các cá nhân đã được đào tạo chuyên ngành an ninh mạng.

3. 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. Kiến thức, kỹ năng chuyên sâu về an ninh mạng gồm:

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 về an ninh mạng do tổ chức nước ngoài cấp, còn hiệu lực và được Bộ Công an công nhận tương đương với kiến thức, 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 trưởng Bộ Công an ban hành khung chương trình tập huấn, chuẩn kiến thức, kỹ năng quy định tại khoản 3, khoản 4 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 trưởng Quốc phòng ban hành khung chương trình tập huấn, chuẩn kiến thức, 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.

8. Việc áp dụng yêu cầu về kiến thức, kỹ năng chuyên sâu về an ninh mạng quy định tại khoản 1 Điều này được thực hiện theo lộ trình sau đây:

a) Cơ quan, tổ chức, doanh nghiệp nhà nước có trách nhiệm rà soát đối tượng đang đảm nhiệm vị trí quy định tại khoản 1 Điều 34 Luật An ninh mạng, bố trí kinh phí, tổ chức tập huấn trong thời hạn 24 tháng kể từ ngày Nghị định này có hiệu lực thi hành;

b) Chủ quản hệ thống thông tin cấp độ 3, cấp độ 4, cấp độ 5 trong cơ quan, tổ chức, doanh nghiệp Nhà nước có trách nhiệm rà soát đối tượng đang đảm nhiệm vị trí quy định tại khoản 2 Điều 34 Luật An ninh mạng thuộc phạm vi quản lý bố trí kinh phí, tổ chức tập huấn trong thời hạn 36 tháng kể từ ngày Nghị định này có hiệu lực thi hành.

**Điều 25. 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 24 và đáp ứng yêu cầu tại Điều 27 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) 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;

b) 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 25 ngày làm việc kể từ ngày kết thúc khóa học;

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

d) 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 26. 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 tham gia Mạng lưới theo Mẫu số 03 Phụ lục ban hành kèm theo Nghị định này;

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, giáo trình, tài liệu nội dung giảng dạy chứng minh 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) Các quyền lợi khác theo quy định của pháp luật.

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 27. 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 28. 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;

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, khoản 2 Điều 34 của Luật An ninh mạng.

**Điều 29. 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 30. Hiệu lực thi hành**

Nghị định này có hiệu lực thi hành từ ngày 19 tháng 8 năm 2026.

**Điều 31. Điều khoản chuyển tiếp**

Hồ sơ đề nghị thẩm định an ninh mạng, hồ sơ đề nghị đánh giá điều kiện an ninh mạng đã được cơ quan có thẩm quyền tiếp nhận hợp lệ theo quy định của Nghị định số 53/2022/NĐ-CP trước ngày Nghị định này có hiệu lực thi hành mà chưa có kết quả giải quyết thì tiếp tục được giải quyết theo quy định của Nghị định số 53/2022/NĐ-CP.

**Điều 32. Trách nhiệm thi hành**

Bộ trưởng, Thủ trưởng cơ quan ngang bộ, Chủ tịch Ủy ban nhân dân các tỉnh, thành phố trực thuộc rung ương và các cơ quan, tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Nghị định này.

**TM. CHÍNH PHỦ**
**KT. THỦ TƯỚNG**
**PHÓ THỦ TƯỚNG**

**Phạm Gia Túc**

**Phụ lục**

*(Kèm theo Nghị định số 333/2026/NĐ-CP ngày 19 tháng 8 năm 2026 của Chính phủ)*

| | |
|---|---|
| Mẫu số 01 | Về việc thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia |
| Mẫu số 02 | Về việc đề nghị chứng nhận điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia |
| Mẫu số 03 | Đơn đăng ký tham gia mạng lưới tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng |

**Mẫu số 01**

| | |
|---|---|
| **CƠ QUAN, TỔ CHỨC**<br>_____<br>Số: ……<br>V/v thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**<br>**Độc lập - Tự do - Hạnh phúc**<br>_____<br>*……, 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 và biện pháp thi hành 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) Hồ sơ thiết kế chi tiết dự án đầu tư xây dựng mới, nâng cấp, mở rộng hệ thống thông tin; đề án, kế hoạch, phương án nâng cấp, mở rộng hệ thống thông tin;

b) Tài liệu thể hiện kết quả xác định cấp độ an ninh mạng của hệ thống thông tin;

c) Tài liệu khác có liên quan đến nội dung đề nghị thẩm định, nếu có.

| | |
|---|---|
| ***Nơi nhận:***<br>- Như trên;<br>- …… | **ĐẠI DIỆN CƠ QUAN, TỔ CHỨC**<br>*(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 5 Điều 5 của Nghị định này.

[2] Tên cơ quan, đơn vị.

**Mẫu số 02**

| | |
|---|---|
| **CƠ QUAN, TỔ CHỨC**<br>_____<br>Số: ……<br>V/v đề nghị chứng nhận điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**<br>**Độc lập - Tự do - Hạnh phúc**<br>_____<br>*……, 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 và biện pháp thi hành 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 khả thi, hồ sơ thiết kế kỹ thuật, hồ sơ thiết kế thi công hoặc tài liệu tương đương của dự án đầu tư xây dựng, nâng cấp, mở rộng hệ thống thông tin;

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

c) Tài liệu thể hiện kết quả thẩm định an ninh mạng, nếu có;

d) Tài liệu khác có liên quan đến nội dung đề nghị đánh giá, nếu có.

| | |
|---|---|
| ***Nơi nhận:***<br>- Như trên;<br>- …… | **ĐẠI DIỆN CƠ QUAN, TỔ CHỨC**<br>*(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 5 Điều 6 của Nghị định này.
[2] Tên cơ quan, đơn vị.

**Mẫu số 03**

| | |
|---|---|
| **CƠ QUAN, TỔ CHỨC** | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** |
| _____ | **Độc lập - Tự do - Hạnh phúc** |
| Số: …… | *……, ngày ... tháng ... năm ...* |

**ĐƠN ĐĂNG KÝ THAM GIA MẠNG LƯỚI TẬP HUẤN KIẾN THỨC, KỸ NĂNG CHUYÊN SÂU VỀ AN NINH MẠNG**

Kính gửi: ……

**I. THÔNG TIN VỀ CƠ SỞ TẬP HUẤN**

- Tên đầy đủ của cơ quan: *[Ghi tên đầy đủ]*
- Mã số thuế *(nếu có): ...*
- Tên tiếng Anh: *[Ghi tên tiếng Anh (nếu có)]*
- Địa chỉ: *[Ghi địa chỉ của cơ quan]*
- Điện thoại: *[Ghi số điện thoại liên lạc]*
- E-mail: *[Ghi địa chỉ hộp thư điện tử]*
- Website: *[Ghi địa chỉ trang thông tin điện tử của cơ quan (nếu có)]*
- Đại diện pháp nhân: *[Ghi tên người đại diện theo pháp luật]*
- Thông tin đầu mối liên lạc: *[Ghi thông tin Họ và tên, Chức vụ, số điện thoại, email liên hệ]*

**II. GIỚI THIỆU VỀ NĂNG LỰC TẬP HUẤN**

*Cơ sở tập huấn giới thiệu về: cơ sở vật chất; đội ngũ giảng viên (số lượng, trình độ, kèm danh sách cụ thể, lĩnh vực đào tạo) ; giáo trình, tài liệu;kinh nghiệm tập huấn.*

**III. HỒ SƠ GỬI KÈM**

- Tài liệu chứng minh việc thành lập và hoạt động hợp pháp.
- Hồ sơ năng lực của cơ sở (tài liệu chứng minh điều kiện về cơ sở vật chất, giảng viên, giáo trình, tài liệu bảo đảm hoạt động tập huấn).
- Các tài liệu khác (nếu có).

**IV. CAM KẾT**

*Chúng tôi cam kết thông tin khai báo trong hồ sơ là chính xác và tuân thủ trách nhiệm, quyền hạn của thành viên mạng lưới và hướng dẫn của Bộ Công an.*

*....., ngày..... tháng..... năm .....*
**NGƯỜI ĐẠI DIỆN THEO PHÁP LUẬT**
*(Ký tên và đóng dấu)*