

UBND TỈNH ĐỒNG NAI
SỞ TƯ PHÁP
២២២★២២២



HỎI - ĐÁP
LUẬT AN NINH MẠNG

LỜI MỞ ĐẦU

Luật An ninh mạng được Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam khóa XIV thông qua tại kỳ họp thứ 5, ngày 12/6/2018 và có hiệu lực thi hành kể từ ngày 01/01/2019, gồm có 7 chương, 43 điều, quy định những nội dung cơ bản về bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; phòng ngừa, xử lý hành vi xâm phạm an ninh mạng; triển khai hoạt động bảo vệ an ninh mạng và quy định trách nhiệm của cơ quan, tổ chức, cá nhân.

Nhằm tuyên truyền, phổ biến những quy định của Luật An ninh mạng đến cán bộ, công chức, viên chức và nhân dân, nâng cao nhận thức pháp luật, hạn chế vi phạm pháp luật, bảo vệ quyền và lợi ích hợp pháp của người dân, Sở Tư pháp tỉnh Đồng Nai biên soạn tài liệu “Hỏi – Đáp Luật An ninh mạng”.

Sở Tư pháp trân trọng giới thiệu!

1. Câu hỏi: An ninh mạng là gì?

Đáp:

Khoản 1 Điều 2 Luật An ninh mạng quy định:

An ninh mạng là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

2. Câu hỏi: Không gian mạng là gì?

Đáp:

Khoản 3 Điều 2 Luật An ninh mạng quy định:

Không gian mạng là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu; là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian.

3. Câu hỏi: Cơ sở hạ tầng không gian mạng quốc gia là gì?

Đáp:

Khoản 5 Điều 2 Luật An ninh mạng quy định:

Cơ sở hạ tầng không gian mạng quốc gia là hệ thống cơ sở vật chất, kỹ thuật để tạo lập, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên không gian mạng quốc gia, bao gồm:

a) Hệ thống truyền dẫn bao gồm hệ thống truyền dẫn quốc gia, hệ thống truyền dẫn kết nối quốc tế, hệ thống vệ tinh, hệ thống truyền dẫn của doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng;

b) Hệ thống các dịch vụ lõi bao gồm hệ thống phân luồng và điều hướng thông tin quốc gia, hệ thống phân giải tên miền

quốc gia (DNS), hệ thống chứng thực quốc gia (PKI/CA) và hệ thống cung cấp dịch vụ kết nối, truy cập Internet của doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng;

c) Dịch vụ, ứng dụng công nghệ thông tin bao gồm dịch vụ trực tuyến; ứng dụng công nghệ thông tin có kết nối mạng phục vụ quản lý, điều hành của cơ quan, tổ chức, tập đoàn kinh tế, tài chính quan trọng; cơ sở dữ liệu quốc gia.

Dịch vụ trực tuyến bao gồm chính phủ điện tử, thương mại điện tử, trang thông tin điện tử, diễn đàn trực tuyến, mạng xã hội, blog;

d) Cơ sở hạ tầng công nghệ thông tin của đô thị thông minh, Internet vạn vật, hệ thống phức hợp thực - ảo, điện toán đám mây, hệ

thống dữ liệu lớn, hệ thống dữ liệu nhanh và hệ thống trí tuệ nhân tạo.

4. Câu hỏi: Bảo vệ an ninh mạng là gì?

Đáp:

Khoản 2 Điều 2 Luật An ninh mạng quy định:

Bảo vệ an ninh mạng là phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi xâm phạm an ninh mạng.

5. Câu hỏi: Chính sách của Nhà nước về an ninh mạng quy định như thế nào?

Đáp:

Điều 3 Luật An ninh mạng quy định về chính sách của Nhà nước về an ninh mạng như sau:

1. Ưu tiên bảo vệ an ninh mạng trong quốc phòng, an ninh, phát triển kinh tế - xã hội, khoa học, công nghệ và đối ngoại.

2. Xây dựng không gian mạng lành mạnh, không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

3. Ưu tiên nguồn lực xây dựng lực lượng chuyên trách bảo vệ an ninh mạng; nâng cao năng lực cho lực lượng bảo vệ an ninh mạng và tổ chức, cá nhân tham gia bảo vệ an ninh mạng; ưu tiên đầu tư cho nghiên cứu, phát triển khoa học, công nghệ để bảo vệ an ninh mạng.

4. Khuyến khích, tạo điều kiện để tổ chức, cá nhân tham gia bảo vệ an ninh mạng, xử lý các nguy cơ đe dọa an ninh mạng; nghiên cứu, phát triển công nghệ, sản phẩm, dịch vụ, ứng dụng nhằm bảo vệ an ninh mạng; phối hợp với cơ quan chức năng trong bảo vệ an ninh mạng.

5. Tăng cường hợp tác quốc tế về an

ninh mạng.

6. Câu hỏi: Nguyên tắc bảo vệ an ninh mạng quy định như thế nào?

Đáp:

Điều 4 Luật An ninh mạng quy định bảo vệ an ninh mạng phải đảm bảo những nguyên tắc sau:

1. Tuân thủ 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. Đặt dưới sự lãnh đạo của Đảng Cộng sản Việt Nam, sự quản lý thống nhất của Nhà nước; huy động sức mạnh tổng hợp của hệ thống chính trị và toàn dân tộc; phát huy vai trò nòng cốt của lực lượng chuyên trách bảo vệ an ninh mạng.

3. Kết hợp chặt chẽ giữa nhiệm vụ bảo vệ an ninh mạng, bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia với nhiệm vụ

phát triển kinh tế - xã hội, bảo đảm quyền con người, quyền công dân, tạo điều kiện cho cơ quan, tổ chức, cá nhân hoạt động trên không gian mạng.

4. Chủ động phòng ngừa, phát hiện, ngăn chặn, đấu tranh, làm thất bại mọi hoạt động sử dụng 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; sẵn sàng ngăn chặn các nguy cơ đe dọa an ninh mạng.

5. Triển khai hoạt động bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia; áp dụng các biện pháp bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia.

6. Hệ thống thông tin quan trọng về an ninh quốc gia được thẩm định, chứng nhận đủ điều kiện về an ninh mạng trước khi đưa

vào vận hành, sử dụng; thường xuyên kiểm tra, giám sát về an ninh mạng trong quá trình sử dụng và kịp thời ứng phó, khắc phục sự cố an ninh mạng.

7. Mọi hành vi vi phạm pháp luật về an ninh mạng phải được xử lý kịp thời, nghiêm minh.

7. Câu hỏi: Bảo vệ an ninh mạng bao gồm những biện pháp nào?

Đáp:

Khoản 1 Điều 5 Luật An ninh mạng quy định bảo vệ an ninh mạng bao gồm những biện pháp sau:

- a) Thẩm định an ninh mạng;
- b) Đánh giá điều kiện an ninh mạng;
- c) Kiểm tra an ninh mạng;
- d) Giám sát an ninh mạng;
- đ) Ứng phó, khắc phục sự cố an ninh mạng;

e) Đấu tranh bảo vệ an ninh mạng;

g) Sử dụng mật mã để bảo vệ thông tin mạng;

h) Ngăn chặn, yêu cầu tạm ngừng, ngừng cung cấp thông tin mạng; đình chỉ, tạm đình chỉ các hoạt động thiết lập, cung cấp và sử dụng mạng viễn thông, mạng Internet, sản xuất và sử dụng thiết bị phát, thu phát sóng vô tuyến theo quy định của pháp luật;

i) Yêu cầu xóa bỏ, truy cập 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;

k) 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;

l) Phong tỏa, hạn chế hoạt động của hệ thống thông tin; 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;

m) Khởi tố, điều tra, truy tố, xét xử theo quy định của Bộ luật Tố tụng hình sự;

n) Biện pháp khác theo quy định của pháp luật về an ninh quốc gia, pháp luật về xử lý vi phạm hành chính.

8. Câu hỏi: Hợp tác quốc tế về an ninh mạng bao gồm những nội dung nào?

Đáp:

Khoản 2 Điều 7 Luật An ninh mạng quy định hợp tác quốc tế về an ninh mạng bao gồm những nội dung sau:

a) Nghiên cứu, phân tích xu hướng an ninh mạng;

b) Xây dựng cơ chế, chính sách nhằm

đẩy mạnh hợp tác giữa tổ chức, cá nhân Việt Nam với tổ chức, cá nhân nước ngoài, tổ chức quốc tế hoạt động về an ninh mạng;

c) Chia sẻ thông tin, kinh nghiệm; hỗ trợ đào tạo, trang thiết bị, công nghệ bảo vệ an ninh mạng;

d) Phòng, chống tội phạm mạng, hành vi xâm phạm an ninh mạng; ngăn ngừa các nguy cơ đe dọa an ninh mạng;

đ) Tư vấn, đào tạo và phát triển nguồn nhân lực an ninh mạng;

e) Tổ chức hội nghị, hội thảo và diễn đàn quốc tế về an ninh mạng;

g) Ký kết và thực hiện điều ước quốc tế, thỏa thuận quốc tế về an ninh mạng;

h) Thực hiện chương trình, dự án hợp tác quốc tế về an ninh mạng;

i) Hoạt động hợp tác quốc tế khác về an ninh mạng.

9. Câu hỏi: Những hành vi nào bị cấm trên không gian mạng?

Đáp:

Căn cứ Điều 13, các khoản 1, 2, 3, 4, 5 Điều 16 và khoản 1 Điều 17, khoản 1 Điều 18 Luật An ninh mạng thì các hành vi bị cấm trên không gian mạng bao gồm:

1. Sử dụng không gian mạng để thực hiện các hành vi:

a) Các hành vi quy định tại khoản 1 Điều 18 của Luật An ninh mạng gồm:

- Đăng tải, phát tán thông tin trên không gian mạng có nội dung xấu ảnh hưởng đến quyền và lợi ích hợp pháp của cá nhân, tổ chức hoặc nhà nước.

- Chiếm đoạt tài sản; tổ chức đánh bạc, đánh bạc qua mạng Internet; trộm cắp cước viễn thông quốc tế trên nền Internet; vi phạm bản quyền và sở hữu trí tuệ trên không gian mạng;

- Giả mạo trang thông tin điện tử của cơ quan, tổ chức, cá nhân; làm giả, lưu hành, trộm cắp, mua bán, thu thập, trao đổi trái phép thông tin thẻ tín dụng, tài khoản ngân hàng của người khác; phát hành, cung cấp, sử dụng trái phép các phương tiện thanh toán;

- Tuyên truyền, quảng cáo, mua bán hàng hóa, dịch vụ thuộc danh mục cấm theo quy định của pháp luật;

- Hướng dẫn người khác thực hiện hành vi vi phạm pháp luật;

- Hành vi khác sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội.

b) Tổ chức, hoạt động, câu kết, xúi giục, mua chuộc, lừa gạt, lôi kéo, đào tạo, huấn luyện người chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam;

c) Xuyên tạc lịch sử, phủ nhận thành tựu cách mạng, phá hoại khối đại đoàn kết toàn dân tộc, xúc phạm tôn giáo, phân biệt đối xử về giới, phân biệt chủng tộc;

d) Thông tin sai sự thật gây hoang mang trong Nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác;

đ) Hoạt động mại dâm, tệ nạn xã hội, mua bán người; đăng tải thông tin dâm ô, đồi trụy, tội ác; phá hoại thuần phong, mỹ tục của dân tộc, đạo đức xã hội, sức khỏe của cộng đồng;

e) Xúi giục, lôi kéo, kích động người khác phạm tội.

2. Thực hiện tấn công mạng, khủng bố mạng, gián điệp mạng, tội phạm mạng; gây sự cố, tấn công, xâm nhập, chiếm quyền điều

khiến, làm sai lệch, gián đoạn, ngưng trệ, tê liệt hoặc phá hoại hệ thống thông tin quan trọng về an ninh quốc gia.

3. Sản xuất, đưa vào sử dụng công cụ, phương tiện, phần mềm hoặc có hành vi cản trở, gây rối loạn hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; phát tán chương trình tin học gây hại cho hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; xâm nhập trái phép vào mạng viễn thông, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử của người khác.

4. Chống lại hoặc cản trở hoạt động của lực lượng bảo vệ an ninh mạng; tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng biện

pháp bảo vệ an ninh mạng.

5. Lợi dụng hoặc lạm dụng hoạt động bảo vệ an ninh mạng để xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân hoặc để trục lợi.

6. Các hành vi khác vi phạm quy định của Luật An ninh mạng.

10. Câu hỏi: Những hành vi vi phạm pháp luật về an ninh mạng bị xử lý như thế nào?

Đáp:

Điều 9 Luật An ninh mạng quy định:

Người nào có hành vi vi phạm quy định của Luật này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật, xử lý vi phạm hành chính hoặc bị truy cứu trách nhiệm hình sự, nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật.

11. Câu hỏi: Hệ thống thông tin quan trọng về an ninh quốc gia được quy định như thế nào?

Đáp:

Điều 10 Luật An ninh mạng quy định:

1. Hệ thống thông tin quan trọng về an ninh quốc gia là hệ thống thông tin khi bị sự cố, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại sẽ xâm phạm nghiêm trọng an ninh mạng.

2. Hệ thống thông tin quan trọng về an ninh quốc gia bao gồm:

a) Hệ thống thông tin quân sự, an ninh, ngoại giao, cơ yếu;

b) Hệ thống thông tin lưu trữ, xử lý thông tin thuộc bí mật nhà nước;

c) Hệ thống thông tin phục vụ lưu giữ, bảo quản hiện vật, tài liệu có giá trị đặc biệt

quan trọng;

d) Hệ thống thông tin phục vụ bảo quản vật liệu, chất đặc biệt nguy hiểm đối với con người, môi trường sinh thái;

đ) Hệ thống thông tin phục vụ bảo quản, chế tạo, quản lý cơ sở vật chất đặc biệt quan trọng khác liên quan đến an ninh quốc gia;

e) Hệ thống thông tin quan trọng phục vụ hoạt động của cơ quan, tổ chức ở trung ương;

g) Hệ thống thông tin quốc gia thuộc lĩnh vực năng lượng, tài chính, ngân hàng, viễn thông, giao thông vận tải, tài nguyên và môi trường, hóa chất, y tế, văn hóa, báo chí;

h) Hệ thống điều khiển và giám sát tự động tại công trình quan trọng liên quan đến an ninh quốc gia, mục tiêu quan trọng về an ninh quốc gia.

12. Câu hỏi: Thông tin trên không gian mạng có nội dung tuyên truyền chống Nhà

nước Cộng hòa xã hội chủ nghĩa Việt Nam là những thông tin như thế nào?

Đáp:

Khoản 1 Điều 16 Luật An ninh mạng quy định thông tin trên không gian mạng có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam bao gồm:

a) Tuyên truyền xuyên tạc, phỉ báng chính quyền nhân dân;

b) Chiến tranh tâm lý, kích động chiến tranh xâm lược, chia rẽ, gây thù hận giữa các dân tộc, tôn giáo và nhân dân các nước;

c) Xúc phạm dân tộc, quốc kỳ, quốc huy, quốc ca, vĩ nhân, lãnh tụ, danh nhân, anh hùng dân tộc.

13. Câu hỏi: Thông tin trên không gian mạng có nội dung kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng là những thông tin như thế nào?

Đáp:

Khoản 2 Điều 16 Luật An ninh mạng quy định thông tin trên không gian mạng có nội dung kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng bao gồm những thông tin:

a) Kêu gọi, vận động, xúi giục, đe dọa, gây chia rẽ, tiến hành hoạt động vũ trang hoặc dùng bạo lực nhằm chống chính quyền nhân dân;

b) Kêu gọi, vận động, xúi giục, đe dọa, lôi kéo tụ tập đông người gây rối, chống người thi hành công vụ, cản trở hoạt động của cơ quan, tổ chức gây mất ổn định về an ninh, trật tự.

14. Câu hỏi: Thông tin trên không gian mạng có nội dung làm nhục, vu khống là những thông tin như thế nào?

Đáp:

Khoản 3 Điều 16 Luật An ninh mạng quy định thông tin trên không gian mạng có nội dung làm nhục, vu khống bao gồm những thông tin:

a) Xúc phạm nghiêm trọng danh dự, uy tín, nhân phẩm của người khác;

b) Thông tin bịa đặt, sai sự thật xâm phạm danh dự, uy tín, nhân phẩm hoặc gây thiệt hại đến quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác.

15. Câu hỏi: Thông tin trên không gian mạng có nội dung xâm phạm trật tự quản lý kinh tế là những thông tin như thế nào?

Đáp:

Khoản 4 Điều 16 Luật An ninh mạng quy định thông tin trên không gian mạng có nội dung xâm phạm trật tự quản lý kinh tế bao gồm:

a) Thông tin bịa đặt, sai sự thật về sản phẩm, hàng hóa, tiền, trái phiếu, tín phiếu,

công trái, séc và các loại giấy tờ có giá khác;

b) Thông tin bịa đặt, sai sự thật trong lĩnh vực tài chính, ngân hàng, thương mại điện tử, thanh toán điện tử, kinh doanh tiền tệ, huy động vốn, kinh doanh đa cấp, chứng khoán.

16. Câu hỏi: Hành vi gián điệp mạng; xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng bao gồm những hành vi nào?

Đáp:

Khoản 1 Điều 17 Luật An ninh mạng quy định hành vi gián điệp mạng; xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng bao gồm:

a) Chiếm đoạt, mua bán, thu giữ, cố ý làm lộ thông tin thuộc bí mật nhà nước, bí

mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư gây ảnh hưởng đến danh dự, uy tín, nhân phẩm, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân;

b) Cố ý xóa, làm hư hỏng, thất lạc, thay đổi thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư được truyền đưa, lưu trữ trên không gian mạng;

c) Cố ý thay đổi, hủy bỏ hoặc làm vô hiệu hóa biện pháp kỹ thuật được xây dựng, áp dụng để bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư;

d) Đưa lên không gian mạng những thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật

gia đình và đời sống riêng tư trái quy định của pháp luật;

đ) Cố ý nghe, ghi âm, ghi hình trái phép các cuộc đàm thoại;

e) Hành vi khác cố ý xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư.

17. Câu hỏi: Chủ quản hệ thống thông tin có trách nhiệm như thế nào trong việc phòng, chống gián điệp mạng; bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng?

Đáp:

Khoản 2 Điều 17 Luật An ninh mạng quy định chủ quản hệ thống thông tin có trách nhiệm sau đây:

a) Kiểm tra an ninh mạng nhằm phát hiện, loại bỏ mã độc, phần cứng độc hại, khắc phục điểm yếu, lỗ hổng bảo mật; phát hiện, ngăn chặn và xử lý các hoạt động xâm nhập bất hợp pháp hoặc nguy cơ khác đe dọa an ninh mạng;

b) Triển khai biện pháp quản lý, kỹ thuật để phòng ngừa, phát hiện, ngăn chặn hành vi gián điệp mạng, xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên hệ thống thông tin và kịp thời gỡ bỏ thông tin liên quan đến hành vi này;

c) Phối hợp, thực hiện yêu cầu của lực lượng chuyên trách an ninh mạng về phòng, chống gián điệp mạng, bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên hệ thống thông tin.

18. Câu hỏi: Phòng, chống hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội được quy định như thế nào?

Đáp:

Điều 18 Luật An ninh mạng quy định:

1. Hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội bao gồm:

a) Đăng tải, phát tán thông tin xấu xâm phạm đến quyền và lợi ích hợp pháp của cá nhân, tổ chức hoặc lợi ích quốc gia, dân tộc theo quy định của Luật An ninh mạng;

b) Chiếm đoạt tài sản; tổ chức đánh bạc, đánh bạc qua mạng Internet; trộm cắp cước viễn thông quốc tế trên nền Internet; vi phạm bản quyền và sở hữu trí tuệ trên không

gian mạng;

c) Giả mạo trang thông tin điện tử của cơ quan, tổ chức, cá nhân; làm giả, lưu hành, trộm cắp, mua bán, thu thập, trao đổi trái phép thông tin thẻ tín dụng, tài khoản ngân hàng của người khác; phát hành, cung cấp, sử dụng trái phép các phương tiện thanh toán;

d) Tuyên truyền, quảng cáo, mua bán hàng hóa, dịch vụ thuộc danh mục cấm theo quy định của pháp luật;

đ) Hướng dẫn người khác thực hiện hành vi vi phạm pháp luật;

e) Hành vi khác sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội.

19. Câu hỏi: Hành vi tấn công mạng và hành vi có liên quan đến tấn công mạng bao gồm những hành vi nào?

Đáp:

Khoản 1 Điều 19 Luật An ninh mạng quy định hành vi tấn công mạng và hành vi có liên quan đến tấn công mạng bao gồm:

a) Phát tán chương trình tin học gây hại cho mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử;

b) Gây cản trở, rối loạn, làm tê liệt, gián đoạn, ngưng trệ hoạt động, ngăn chặn trái phép việc truyền đưa dữ liệu của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử;

c) Xuyên nhập, làm tổn hại, chiếm đoạt dữ liệu được lưu trữ, truyền đưa qua mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều

khiển thông tin, cơ sở dữ liệu, phương tiện điện tử;

d) Xâm nhập, tạo ra hoặc khai thác điểm yếu, lỗ hổng bảo mật và dịch vụ hệ thống để chiếm đoạt thông tin, thu lợi bất chính;

đ) Sản xuất, mua bán, trao đổi, tặng cho công cụ, thiết bị, phần mềm có tính năng tấn công mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử để sử dụng vào mục đích trái pháp luật;

e) Hành vi khác gây ảnh hưởng đến hoạt động bình thường của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử.

20. Câu hỏi: Lực lượng chuyên trách bảo vệ an ninh mạng có trách nhiệm

như thế nào trong việc phòng, chống tấn công mạng?

Đáp:

Khoản 3 Điều 19 Luật An ninh mạng quy định:

Khi xảy ra tấn công mạng xâm phạm hoặc đe dọa xâm phạm chủ quyền, lợi ích, an ninh quốc gia, gây tổn hại nghiêm trọng trật tự, an toàn xã hội, lực lượng chuyên trách bảo vệ an ninh mạng chủ trì, phối hợp với chủ quản hệ thống thông tin và tổ chức, cá nhân có liên quan áp dụng biện pháp xác định nguồn gốc tấn công mạng, thu thập chứng cứ; yêu cầu doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng chặn lọc thông tin để ngăn chặn, loại trừ hành vi tấn công mạng và cung cấp đầy đủ, kịp thời thông tin, tài liệu liên quan.

21. Câu hỏi: Tình huống nguy hiểm về an ninh mạng bao gồm những gì?

Đáp:

Khoản 1 Điều 21 Luật An ninh mạng quy định tình huống nguy hiểm về an ninh mạng bao gồm:

a) Xuất hiện thông tin kích động trên không gian mạng có nguy cơ xảy ra bạo loạn, phá rối an ninh, khủng bố;

b) Tấn công vào hệ thống thông tin quan trọng về an ninh quốc gia;

c) Tấn công nhiều hệ thống thông tin trên quy mô lớn, cường độ cao;

d) Tấn công mạng nhằm phá hủy công trình quan trọng về an ninh quốc gia, mục tiêu quan trọng về an ninh quốc gia;

đ) Tấn công mạng xâm phạm nghiêm trọng chủ quyền, lợi ích, an ninh quốc gia; gây tổn hại đặc biệt nghiêm trọng trật tự, an

toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

22. Câu hỏi: Trách nhiệm phòng ngừa tình huống nguy hiểm về an ninh mạng được quy định như thế nào?

Đáp:

Khoản 2 Điều 21 Luật An ninh mạng quy định về trách nhiệm phòng ngừa tình huống nguy hiểm về an ninh mạng như sau:

a) Lực lượng chuyên trách bảo vệ an ninh mạng phối hợp với chủ quản hệ thống thông tin quan trọng về an ninh quốc gia triển khai các giải pháp kỹ thuật, nghiệp vụ để phòng ngừa, phát hiện, xử lý tình huống nguy hiểm về an ninh mạng;

b) Doanh nghiệp viễn thông, Internet, công nghệ thông tin, doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng

và cơ quan, tổ chức, cá nhân có liên quan có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an trong phòng ngừa, phát hiện, xử lý tình huống nguy hiểm về an ninh mạng.

23. Câu hỏi: Việc xử lý tình huống nguy hiểm về an ninh mạng bao gồm những biện pháp nào?

Đáp:

Khoản 3 Điều 21 Luật An ninh mạng quy định biện pháp xử lý tình huống nguy hiểm về an ninh mạng bao gồm:

a) Triển khai ngay phương án phòng ngừa, ứng phó khẩn cấp về an ninh mạng, ngăn chặn, loại trừ hoặc giảm nhẹ thiệt hại do tình huống nguy hiểm về an ninh mạng gây ra;

b) Thông báo đến cơ quan, tổ chức, cá nhân có liên quan;

c) Thu thập thông tin liên quan; theo dõi, giám sát liên tục đối với tình huống nguy hiểm về an ninh mạng;

d) Phân tích, đánh giá thông tin, dự báo khả năng, phạm vi ảnh hưởng và mức độ thiệt hại do tình huống nguy hiểm về an ninh mạng gây ra;

đ) Ngừng cung cấp thông tin mạng tại khu vực cụ thể hoặc ngắt công kết nối mạng quốc tế;

e) Bố trí lực lượng, phương tiện ngăn chặn, loại bỏ tình huống nguy hiểm về an ninh mạng;

g) Biện pháp khác theo quy định của Luật An ninh quốc gia.

24. Câu hỏi: Hoạt động đấu tranh bảo vệ an ninh mạng được quy định như thế nào?

Đáp:

Điều 22 Luật An ninh mạng quy định:

1. Đấu tranh bảo vệ an ninh mạng là hoạt động có tổ chức do lực lượng chuyên trách bảo vệ an ninh mạng thực hiện trên không gian mạng nhằm bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội.

2. Nội dung đấu tranh bảo vệ an ninh mạng bao gồm:

a) Tổ chức nắm tình hình có liên quan đến hoạt động bảo vệ an ninh quốc gia;

b) Phòng, chống tấn công và bảo vệ hoạt động ổn định của hệ thống thông tin quan trọng về an ninh quốc gia;

c) Làm tê liệt hoặc hạn chế hoạt động sử dụng không gian mạng nhằm gây phương hại an ninh quốc gia hoặc gây tổn hại đặc biệt nghiêm trọng trật tự, an toàn xã hội;

d) Chủ động tấn công vô hiệu hóa mục tiêu trên không gian mạng nhằm bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn

xã hội.

3. Bộ Công an chủ trì, phối hợp với Bộ, ngành có liên quan thực hiện đấu tranh bảo vệ an ninh mạng.

25. Câu hỏi: Triển khai hoạt động bảo vệ an ninh mạng trong cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương được quy định như thế nào?

Đáp:

Điều 23 Luật An ninh mạng quy định về triển khai hoạt động bảo vệ an ninh mạng trong cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương như sau:

1. Nội dung triển khai hoạt động bảo vệ an ninh mạng bao gồm:

a) Xây dựng, hoàn thiện quy định, quy chế sử dụng mạng máy tính nội bộ, mạng máy tính có kết nối mạng Internet; phương án bảo đảm an ninh mạng đối với hệ thống

thông tin; phương án ứng phó, khắc phục sự cố an ninh mạng;

b) Ứng dụng, triển khai phương án, biện pháp, công nghệ bảo vệ an ninh mạng đối với hệ thống thông tin và thông tin, tài liệu được lưu trữ, soạn thảo, truyền đưa trên hệ thống thông tin thuộc phạm vi quản lý;

c) Tổ chức bồi dưỡng kiến thức về an ninh mạng cho cán bộ, công chức, viên chức, người lao động; nâng cao năng lực bảo vệ an ninh mạng cho lực lượng bảo vệ an ninh mạng;

d) Bảo vệ an ninh mạng trong hoạt động cung cấp dịch vụ công trên không gian mạng, cung cấp, trao đổi, thu thập thông tin với cơ quan, tổ chức, cá nhân, chia sẻ thông tin trong nội bộ và với cơ quan khác hoặc trong hoạt động khác theo quy định của Chính phủ;

đ) Đầu tư, xây dựng hạ tầng cơ sở vật

chất phù hợp với điều kiện bảo đảm triển khai hoạt động bảo vệ an ninh mạng đối với hệ thống thông tin;

e) Kiểm tra an ninh mạng đối với hệ thống thông tin; phòng, chống hành vi vi phạm pháp luật về an ninh mạng; ứng phó, khắc phục sự cố an ninh mạng.

2. Người đứng đầu cơ quan, tổ chức có trách nhiệm triển khai hoạt động bảo vệ an ninh mạng thuộc quyền quản lý.

26. Câu hỏi: Kiểm tra an ninh mạng đối với hệ thống thông tin của cơ quan, tổ chức không thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia được thực hiện trong trường hợp nào?

Đáp:

Khoản 1 Điều 24 Luật An ninh mạng quy định kiểm tra an ninh mạng đối với hệ thống thông tin của cơ quan, tổ chức không thuộc

Danh mục hệ thống thông tin quan trọng về an ninh quốc gia trong trường hợp sau đây:

a) Khi có hành vi vi phạm pháp luật về an ninh mạng xâm phạm an ninh quốc gia hoặc gây tổn hại nghiêm trọng trật tự, an toàn xã hội;

b) Khi có đề nghị của chủ quản hệ thống thông tin.

27. Câu hỏi: Đối tượng kiểm tra an ninh mạng đối với hệ thống thông tin của cơ quan, tổ chức không thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia bao gồm?

Đáp:

Khoản 2 Điều 24 Luật An ninh mạng quy định đối tượng kiểm tra an ninh mạng bao gồm:

a) Hệ thống phần cứng, phần mềm, thiết bị số được sử dụng trong hệ thống thông tin;

b) Thông tin được lưu trữ, xử lý, truyền

đưa trong hệ thống thông tin;

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

28. Câu hỏi: Bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia, công kết nối mạng quốc tế được quy định như thế nào?

Đáp:

Điều 25 Luật An ninh mạng quy định:

1. Bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia, công kết nối mạng quốc tế phải bảo đảm kết hợp chặt chẽ giữa yêu cầu bảo vệ an ninh mạng với yêu cầu phát triển kinh tế - xã hội; khuyến khích công kết nối quốc tế đặt trên lãnh thổ Việt Nam; khuyến khích tổ chức, cá nhân tham gia đầu tư xây dựng cơ sở hạ tầng không gian mạng quốc gia.

2. Cơ quan, tổ chức, cá nhân quản lý, khai thác cơ sở hạ tầng không gian mạng quốc gia, công kết nối mạng quốc tế có trách nhiệm sau đây:

a) Bảo vệ an ninh mạng thuộc quyền quản lý; chịu sự quản lý, thanh tra, kiểm tra và thực hiện các yêu cầu về bảo vệ an ninh mạng của cơ quan nhà nước có thẩm quyền;

b) Tạo điều kiện, thực hiện các biện pháp kỹ thuật, nghiệp vụ cần thiết để cơ quan nhà nước có thẩm quyền thực hiện nhiệm vụ bảo vệ an ninh mạng khi có đề nghị.

29. Câu hỏi: Trang thông tin điện tử, cổng thông tin điện tử hoặc chuyên trang trên mạng xã hội của cơ quan, tổ chức, cá nhân không được cung cấp, đăng tải, truyền đưa những thông tin nào?

Đáp:

Căn cứ các khoản 1, 2, 3, 4, 5 Điều 16

và khoản 1 Điều 26 Luật An ninh mạng thì Trang thông tin điện tử, Cổng thông tin điện tử hoặc chuyên trang trên mạng xã hội của cơ quan, tổ chức, cá nhân không được cung cấp, đăng tải, truyền đưa những thông tin sau:

1. Thông tin trên không gian mạng có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam bao gồm:

a) Tuyên truyền xuyên tạc, phỉ báng chính quyền nhân dân;

b) Chiến tranh tâm lý, kích động chiến tranh xâm lược, chia rẽ, gây thù hận giữa các dân tộc, tôn giáo và nhân dân các nước;

c) Xúc phạm dân tộc, quốc kỳ, quốc huy, quốc ca, vĩ nhân, lãnh tụ, danh nhân, anh hùng dân tộc.

2. Thông tin có nội dung kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng bao gồm:

a) Kêu gọi, vận động, xúi giục, đe dọa, gây chia rẽ, tiến hành hoạt động vũ trang hoặc dùng bạo lực nhằm chống chính quyền nhân dân;

b) Kêu gọi, vận động, xúi giục, đe dọa, lôi kéo tụ tập đông người gây rối, chống người thi hành công vụ, cản trở hoạt động của cơ quan, tổ chức gây mất ổn định về an ninh, trật tự.

3. Thông tin có nội dung làm nhục, vu khống bao gồm:

a) Xúc phạm nghiêm trọng danh dự, uy tín, nhân phẩm của người khác;

b) Thông tin bịa đặt, sai sự thật xâm phạm danh dự, uy tín, nhân phẩm hoặc gây thiệt hại đến quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác.

4. Thông tin có nội dung xâm phạm trật tự quản lý kinh tế bao gồm:

a) Thông tin bịa đặt, sai sự thật về sản phẩm, hàng hóa, tiền, trái phiếu, tín phiếu, công trái, séc và các loại giấy tờ có giá khác;

b) Thông tin bịa đặt, sai sự thật trong lĩnh vực tài chính, ngân hàng, thương mại điện tử, thanh toán điện tử, kinh doanh tiền tệ, huy động vốn, kinh doanh đa cấp, chứng khoán.

5. Thông tin có nội dung bịa đặt, sai sự thật gây hoang mang trong Nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác.

6. Những thông tin khác có nội dung xâm phạm an ninh quốc gia.

30. Câu hỏi: Doanh nghiệp trong nước và ngoài nước cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia

tăng trên không gian mạng tại Việt Nam có trách nhiệm như thế nào?

Đáp:

Căn cứ khoản 2, 3 Điều 26 Luật An ninh mạng, Doanh nghiệp trong nước và ngoài nước cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng tại Việt Nam có trách nhiệm như sau:

a) Xác thực thông tin khi người dùng đăng ký tài khoản số; bảo mật thông tin, tài khoản của người dùng; cung cấp thông tin người dùng cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an khi có yêu cầu bằng văn bản để phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng;

b) Ngăn chặn việc chia sẻ thông tin, xóa bỏ thông tin có nội dung xấu theo quy định của Luật An ninh mạng trên dịch vụ hoặc hệ

thống thông tin do cơ quan, tổ chức trực tiếp quản lý chậm nhất là 24 giờ kể từ thời điểm có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an hoặc cơ quan có thẩm quyền của Bộ Thông tin và Truyền thông và lưu nhật ký hệ thống để phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng trong thời gian theo quy định của Chính phủ;

c) Không cung cấp hoặc ngừng cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng cho tổ chức, cá nhân đăng tải trên không gian mạng thông tin có nội dung xấu theo quy định của Luật An ninh mạng khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an hoặc cơ quan có thẩm quyền của Bộ Thông tin và Truyền thông.

d) Trường hợp doanh nghiệp có hoạt động thu thập, khai thác, phân tích, xử lý dữ liệu

về thông tin cá nhân, dữ liệu về mối quan hệ của người sử dụng dịch vụ, dữ liệu do người sử dụng dịch vụ tại Việt Nam tạo ra phải lưu trữ dữ liệu này tại Việt Nam trong thời gian theo quy định của Chính phủ. Doanh nghiệp ngoài nước thuộc trường hợp này phải đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam.

31. Câu hỏi: Bảo vệ trẻ em trên không gian mạng được quy định như thế nào?

Đáp:

Điều 29 Luật An ninh mạng quy định:

1. Trẻ em có quyền được bảo vệ, tiếp cận thông tin, tham gia hoạt động xã hội, vui chơi, giải trí, giữ bí mật cá nhân, đời sống riêng tư và các quyền khác khi tham gia trên không gian mạng.

2. Chủ quản hệ thống thông tin, doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng

trên không gian mạng có trách nhiệm kiểm soát nội dung thông tin trên hệ thống thông tin hoặc trên dịch vụ do doanh nghiệp cung cấp để không gây nguy hại cho trẻ em, xâm phạm đến trẻ em, quyền trẻ em; ngăn chặn việc chia sẻ và xóa bỏ thông tin có nội dung gây nguy hại cho trẻ em, xâm phạm đến trẻ em, quyền trẻ em; kịp thời thông báo, phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an để xử lý.

3. Cơ quan, tổ chức, cá nhân tham gia hoạt động trên không gian mạng có trách nhiệm phối hợp với cơ quan có thẩm quyền trong bảo đảm quyền của trẻ em trên không gian mạng, ngăn chặn thông tin có nội dung gây nguy hại cho trẻ em theo quy định của Luật này và pháp luật về trẻ em.

4. Cơ quan, tổ chức, cha mẹ, giáo viên, người chăm sóc trẻ em và cá nhân khác liên quan có trách nhiệm bảo đảm quyền của trẻ

em, bảo vệ trẻ em khi tham gia không gian mạng theo quy định của pháp luật về trẻ em.

5. Lực lượng chuyên trách bảo vệ an ninh mạng và các cơ quan chức năng có trách nhiệm áp dụng biện pháp để phòng ngừa, phát hiện, ngăn chặn, xử lý nghiêm hành vi sử dụng không gian mạng gây nguy hại cho trẻ em, xâm phạm đến trẻ em, quyền trẻ em.

32. Câu hỏi: Lực lượng bảo vệ an ninh mạng được quy định như thế nào?

Đáp:

Điều 30 Luật An ninh mạng quy định:

1. Lực lượng chuyên trách bảo vệ an ninh mạng được bố trí tại Bộ Công an, Bộ Quốc phòng.

2. Lực lượng bảo vệ an ninh mạng được bố trí tại Bộ, ngành, Ủy ban nhân dân cấp tỉnh, cơ quan, tổ chức quản lý trực tiếp hệ thống thông tin quan trọng về an ninh quốc gia.

3. Tổ chức, cá nhân được huy động tham gia bảo vệ an ninh mạng.

33. Câu hỏi: Hoạt động phổ biến kiến thức về an ninh mạng được quy định như thế nào?

Đáp:

Điều 34 Luật An ninh mạng quy định:

1. Nhà nước có chính sách phổ biến kiến thức về an ninh mạng trong phạm vi cả nước, khuyến khích cơ quan nhà nước phối hợp với tổ chức tư nhân, cá nhân thực hiện chương trình giáo dục và nâng cao nhận thức về an ninh mạng.

2. Bộ, ngành, cơ quan, tổ chức có trách nhiệm xây dựng và triển khai hoạt động phổ biến kiến thức về an ninh mạng cho cán bộ, công chức, viên chức, người lao động trong Bộ, ngành, cơ quan, tổ chức.

3. Ủy ban nhân dân cấp tỉnh có trách

nhiệm xây dựng và triển khai hoạt động phổ biến kiến thức, nâng cao nhận thức về an ninh mạng cho cơ quan, tổ chức, cá nhân của địa phương.

34. Câu hỏi: Doanh nghiệp cung cấp dịch vụ trên không gian mạng tại Việt Nam có trách nhiệm như thế nào?

Đáp:

Căn cứ khoản 1 Điều 41 Luật An ninh mạng, doanh nghiệp cung cấp dịch vụ trên không gian mạng tại Việt Nam có trách nhiệm sau đây:

a) Cảnh báo khả năng mất an ninh mạng trong việc sử dụng dịch vụ trên không gian mạng do mình cung cấp và hướng dẫn biện pháp phòng ngừa;

b) Xây dựng phương án, giải pháp phản ứng nhanh với sự cố an ninh mạng, xử lý ngay điểm yếu, lỗ hổng bảo mật, mã độc, tấn

công mạng, xâm nhập mạng và rủi ro an ninh khác; khi xảy ra sự cố an ninh mạng, ngay lập tức triển khai phương án khẩn cấp, biện pháp ứng phó thích hợp, đồng thời báo cáo với lực lượng chuyên trách bảo vệ an ninh mạng theo quy định của Luật An ninh mạng.

c) Áp dụng các giải pháp kỹ thuật và các biện pháp cần thiết khác nhằm bảo đảm an ninh cho quá trình thu thập thông tin, ngăn chặn nguy cơ lộ, lọt, tổn hại hoặc mất dữ liệu; trường hợp xảy ra hoặc có nguy cơ xảy ra sự cố lộ, lọt, tổn hại hoặc mất dữ liệu thông tin người sử dụng, cần lập tức đưa ra giải pháp ứng phó, đồng thời thông báo đến người sử dụng và báo cáo với lực lượng chuyên trách bảo vệ an ninh mạng theo quy định của Luật An ninh mạng.

d) Phối hợp, tạo điều kiện cho lực lượng chuyên trách bảo vệ an ninh mạng trong bảo vệ an ninh mạng.

35. Câu hỏi: Cơ quan, tổ chức, cá nhân sử dụng không gian mạng có trách nhiệm như thế nào?

Đáp:

Điều 42 Luật An ninh mạng quy định cơ quan, tổ chức, cá nhân sử dụng không gian mạng có trách nhiệm như sau:

1. Tuân thủ quy định của pháp luật về an ninh mạng.

2. Kịp thời cung cấp thông tin liên quan đến bảo vệ an ninh mạng, nguy cơ đe dọa an ninh mạng, hành vi xâm phạm an ninh mạng cho cơ quan có thẩm quyền, lực lượng bảo vệ an ninh mạng.

3. Thực hiện yêu cầu và hướng dẫn của cơ quan có thẩm quyền trong bảo vệ an ninh mạng; giúp đỡ, tạo điều kiện cho cơ quan, tổ chức và người có trách nhiệm tiến hành các biện pháp bảo vệ an ninh mạng./.

SỞ TƯ PHÁP TỈNH ĐỒNG NAI

Hỏi - Đáp **Luật An ninh mạng**

Chịu trách nhiệm xuất bản

Võ Thị Xuân Đào

Phó Giám đốc Phụ trách Sở Tư pháp

Ban biên soạn

Võ Thị Xuân Đào

Ngô Văn Toàn

Phan Quang Tuấn

Trần Văn Út

Đông Thị Hoa

~~~~~  
In 3.000 cuốn khổ 10,5 x 14,5 Cm.

In tại Công ty TNHH In L.B.T (0251.393.8888)

Giấy phép xuất bản số: 32/GP-STTTT do Sở Thông tin  
và Truyền thông tỉnh Đồng Nai cấp ngày 01/7/2019

In xong và nộp lưu chiểu tháng 7/2019  
~~~~~


