CỤC AN NINH MẠNG VÀ PHÒNG, CHỐNG TỘI PHẠM
SỬ DỤNG CÔNG NGHỆ CAO - BỘ CÔNG AN

CẨM NANG LUẬT AN NINH MẠNG

HIỂU ĐÚNG LUẬT | NÂNG CAO Ý THỨC | CHỦ ĐỘNG PHÒNG NGỪA | XỬ LÝ NGHIÊM VI PHẠM

MỤC LỤC

I GIỚI THIỆU CHUNG VỀ LUẬT AN NINH MẠNG 1

II NHỮNG NỘI DUNG MỚI TRONG LUẬT AN NINH MẠNG 2

III CÁC ĐIỀU KIỆN BẢO ĐẢM CHO VIỆC THI HÀNH 3

IV TRIỂN KHAI HOẠT ĐỘNG THI HÀNH 4

GIỚI THIỆU CHUNG VỀ LUẬT AN NINH MẠNG

I

I SỰ CẦN THIẾT BAN HÀNH

Luật An ninh mạng 2025 được **Quốc hội khóa XV** thông qua ngày 10/12/2025 và **có hiệu lực từ 01/7/2026**. Luật được ban hành nhằm đáp ứng yêu cầu bảo vệ chủ quyền, an ninh quốc gia, an ninh dữ liệu và an toàn thông tin trong bối cảnh chuyển đổi số và Cách mạng công nghiệp 4.0.

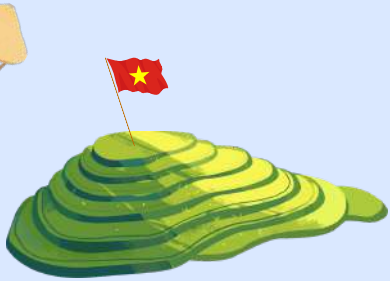
Luật hướng tới thống nhất đầu mối quản lý nhà nước, **khắc phục sự chồng chéo** giữa các cơ quan và giữa Luật An ninh mạng 2018 với Luật An toàn thông tin mạng 2015. Đồng thời, luật xử lý các thách thức mới như tấn công mạng, gián điệp mạng, lộ lọt dữ liệu cá nhân, thông tin xấu độc và tội phạm công nghệ cao xuyên biên giới.

Trên cơ sở kế thừa và hợp nhất các quy định còn phù hợp, **Luật An ninh mạng 2025** xây dựng khuôn khổ pháp lý đồng bộ về bảo vệ hệ thống thông tin quan trọng, tiêu chuẩn kỹ thuật, lực lượng bảo vệ, cơ chế phối hợp và trách nhiệm của các chủ thể; qua đó vừa bảo đảm an ninh mạng, vừa tạo môi trường ổn định cho kinh tế số và chuyển đổi số quốc gia.

I MỤC TIÊU

- Thống nhất và hoàn thiện pháp luật về an ninh mạng
- Khắc phục chồng chéo trong quản lý nhà nước
- Tăng cường phòng ngừa, phát hiện và xử lý sự cố mạng
- Bảo vệ hệ thống thông tin dữ liệu và quyền lợi người dân
- Hài hòa giữa bảo đảm an ninh mạng và phát triển kinh tế số, chuyển đổi số

I QUAN ĐIỂM



Bảo đảm sự lãnh đạo của Đảng, quản lý thống nhất của Nhà nước, phát huy vai trò của toàn dân và lực lượng chuyên trách

Chủ động, tự chủ trong phòng ngừa và ứng phó nguy cơ mạng, đẩy mạnh công nghệ và sản phẩm an ninh mạng "Make in Vietnam".

Kết hợp bảo đảm an ninh mạng với phát triển kinh tế – xã hội, chuyển đổi số và bảo vệ quyền con người, quyền công dân.

Lấy dữ liệu và con người làm trọng tâm, tăng cường bảo vệ dữ liệu, phát triển nhân lực chất lượng cao và nâng cao nhận thức xã hội.

I

BỐ CỤC

Luật An ninh mạng 2025 gồm 08 chương, 45 điều

Chương I: Quy định chung, nguyên tắc, biện pháp bảo vệ an ninh mạng, hợp tác quốc tế và các hành vi bị cấm.

Chương II: Phân loại hệ thống thông tin theo 05 cấp và bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia.

Chương III: Phòng ngừa, phát hiện và xử lý hành vi xâm phạm an ninh mạng; bảo vệ bí mật, trẻ em và phòng, chống tấn công mạng.

Chương IV: Bảo vệ an ninh mạng trong cơ quan, tổ chức; bảo vệ hạ tầng mạng, thông tin và dữ liệu.

I

BỐ CỤC

8 CHƯƠNG **45** ĐIỀU

Chương V: Tiêu chuẩn, quy chuẩn kỹ thuật và điều kiện kinh doanh sản phẩm, dịch vụ an ninh mạng.

Chương VI: Tổ chức lực lượng, phát triển nhân lực, đào tạo, nghiên cứu công nghệ và bảo đảm kinh phí.

Chương VII: Trách nhiệm quản lý của Nhà nước, chủ quản hệ thống, doanh nghiệp cung cấp dịch vụ và người sử dụng mạng.

Chương VIII: Sửa đổi các luật liên quan, quy định hiệu lực từ 01/7/2026 và điều khoản chuyển tiếp.

NEW

NỘI DUNG MỚI TRONG LUẬT AN NINH MẠNG

II

II NỘI DUNG MỚI

NEW

Hoàn thiện và thống nhất hệ thống khái niệm làm nền tảng cho quản lý và bảo vệ an ninh mạng

An ninh mạng: Bao quát sự ổn định, an toàn của không gian mạng, hệ thống thông tin, dữ liệu và các hoạt động trên mạng.

An ninh thông tin mạng: Tập trung bảo đảm tính bảo mật, tính toàn vẹn và tính khả dụng của thông tin.

An ninh dữ liệu: Lần đầu được quy định độc lập, coi dữ liệu là tài nguyên chiến lược cần được bảo vệ và khai thác hiệu quả.

Không gian mạng quốc gia: Khẳng định chủ quyền, quyền tài phán và quyền kiểm soát của Việt Nam trên không gian mạng.

II NỘI DUNG MỚI

NEW

CÁC HÀNH VI BỊ NGHIÊM CẤM

Ngăn chặn lạm dụng AI, Deepfake để giả mạo hình ảnh, video, giọng nói nhằm lừa đảo, vu khống, tống tiền hoặc xâm phạm danh dự.

Phòng, chống xâm phạm an ninh kinh tế, xử lý thông tin sai lệch trong tài chính, ngân hàng, chứng khoán, thương mại điện tử và hoạt động đa cấp.

Kiểm soát các nền tảng, dịch vụ hỗ trợ mô hình trái phép, bao gồm sàn giao dịch tài sản số và hệ sinh thái kinh doanh bất hợp pháp.

Bảo vệ dữ liệu cá nhân và danh tính số, nghiêm cấm thu thập, mua bán, trao đổi hoặc sử dụng trái phép thông tin của người khác.

Ngăn chặn tài khoản và hồ sơ giả, xử lý hành vi mở, mua bán hoặc sử dụng trái phép tài khoản ngân hàng, ví điện tử, chứng khoán và các tài khoản số.

II NỘI DUNG MỚI

CÁC HÀNH VI BỊ NGHIÊM CẤM
Lạm dụng AI, Deepfake

Nhận diện thông tin vi phạm pháp luật, tin giả và cơ chế xử lý trên không gian mạng

- **Điều 7 - Luật An ninh mạng 2025 - Nghiêm cấm hành vi đăng tải, chia sẻ thông tin giả mạo, sai sự thật, deepfake. Đây là bước đột phá trong bảo vệ không gian mạng**
- **Khoản 4 Điều 7 - Luật An toàn thông tin mạng 2015 - Cấm thiết lập hệ thống thông tin giả mạo, lừa đảo**
- **Khoản 4, 6 Điều 6 - Luật Giao dịch điện tử 2023 - Xử lý hành vi giả mạo, làm sai lệch, xóa/hủy dữ liệu trái phép; chiếm đoạt tài khoản, chứng thư điện tử**
- **Điểm b Khoản 1 Điều 40 - Luật Viễn thông 2023 - Trách nhiệm của doanh nghiệp viễn thông trong việc bảo đảm an toàn, bảo vệ người dùng và phối hợp xử lý vi phạm**

II NỘI DUNG MỚI

CÁC HÀNH VI BỊ NGHIÊM CẤM
Lạm dụng AI, Deepfake

Khung pháp lý toàn diện

Luật An toàn thông tin mạng 2015

Đảm bảo an toàn hệ thống bảo vệ dữ liệu
kiểm soát truy cập trái phép.

Luật Giao dịch điện tử 2023

Xác lập giá trị pháp lý của thông điệp dữ liệu, cơ chế xác thực trong môi trường số.

Luật an ninh mạng 2025

Luật Viễn thông 2023

Đặt ra yêu cầu về an toàn dịch vụ, bảo vệ người dùng và phối hợp xử lý vi phạm.

Bộ luật Dân sự 2015

Bảo vệ quyền nhân thân, hình ảnh, danh dự, uy tín, đời sống riêng tư.

Bộ luật Hình sự 2015 (sửa đổi, bổ sung 2017)

Truy cứu trách nhiệm hình sự đối với các hành vi vu khống, làm nhục, xâm phạm dữ liệu.

II NỘI DUNG MỚI

CÁC HÀNH VI BỊ NGHIÊM CẤM
Lạm dụng AI, Deepfake

Các giải pháp cụ thể

Hoàn thiện khung pháp lý

- An ninh mạng
- Bảo vệ dữ liệu cá nhân
- Trách nhiệm của các nền tảng số
- Cơ chế phối hợp xử lý thông tin vi phạm

Ứng dụng công nghệ

- Giám sát, phân tích dữ liệu
- Nhận diện nội dung giả mạo
- Truy xuất nguồn gốc thông tin
- Đánh giá mức độ lan truyền của nội dung vi phạm

Nâng Cao Kỹ Năng Số Của Cá Nhân Và Tổ Chức

- Kiểm chứng thông tin trước khi chia sẻ
- Nhận diện tin giả
- Chủ động bảo vệ dữ liệu cá nhân, hình ảnh, thông tin nhận dạng
- Phòng ngừa nguy cơ bị lợi dụng tạo nội dung giả mạo

Tuyên Truyền Và Nâng Cao Nhận Thức

- Tăng "sức đề kháng" của cộng đồng trước tin giả, sai sự thật
- Phản bác các luận điệu sai trái, thù địch
- Nghiên cứu áp dụng mô hình kiểm chứng tin giả để giảm thiểu thiệt hại

II NỘI DUNG MỚI

Bảo vệ an ninh mạng theo cấp độ đối với hệ thống thông tin

Phân loại hệ thống thông tin theo 05 cấp độ, từ mức ảnh hưởng thấp đến mức gây tổn hại đặc biệt nghiêm trọng đối với an ninh quốc gia.

Áp dụng biện pháp bảo vệ tương xứng theo cấp độ: hệ thống cấp 1–2 được chủ động lựa chọn biện pháp; hệ thống cấp 3–4 phải thực hiện các yêu cầu bảo vệ tối thiểu bắt buộc.

Bảo vệ nghiêm ngặt hệ thống thông tin quan trọng về an ninh quốc gia thông qua thẩm định, chứng nhận, giám sát, kiểm tra định kỳ, báo cáo và ứng phó sự cố.

II NỘI DUNG MỚI

NEW

Bảo vệ an ninh mạng theo cấp độ đối với hệ thống thông tin

Không gian mạng đang đối mặt với nhiều nguy cơ như hoạt động tấn công mạng, gián điệp mạng và lộ, mất bí mật nhà nước.

Việc kiểm soát và bảo vệ dữ liệu chưa tương xứng với giá trị và mức độ khai thác trong nền kinh tế số, dẫn đến tình trạng lộ, mất và xâm phạm dữ liệu cá nhân.

Hoạt động sử dụng công nghệ cao để thực hiện hành vi phạm tội, gây thiệt hại lớn về tài sản cho người dân.

Hoạt động sử dụng công nghệ cao để thực hiện hành vi phạm tội, gây thiệt hại lớn về tài sản cho người dân.

Các cơ quan, tổ chức có trách nhiệm tham mưu, tổ chức thực thi, đôn đốc công tác bảo vệ an ninh mạng và đảm bảo thực hiện các biện pháp bảo vệ an ninh mạng.

II NỘI DUNG MỚI

NEW

Trách nhiệm của doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet và các dịch vụ gia tăng trên không gian mạng tại Việt Nam

1

Xử lý nhanh nội dung vi phạm: Gỡ bỏ, ngăn chặn thông tin hoặc dịch vụ vi phạm trong 24 giờ; trường hợp khẩn cấp liên quan an ninh quốc gia không quá 06 giờ.

2

Chủ động phòng ngừa: Doanh nghiệp phải triển khai biện pháp kỹ thuật để phát hiện, cảnh báo, ngăn chặn và xử lý nội dung xâm phạm an ninh quốc gia, trật tự xã hội.

3

Ngừng cung cấp dịch vụ: Có thể khóa hoặc dừng dịch vụ đối với tổ chức, cá nhân vi phạm nghiêm trọng theo yêu cầu của cơ quan chuyên trách.

4

Ứng cứu và báo cáo sự cố: Xây dựng phương án ứng cứu, cảnh báo người dùng và phối hợp xử lý khi xảy ra sự cố an ninh mạng.

5

Hỗ trợ truy vết, điều tra: Định danh địa chỉ IP, cung cấp thông tin và kết nối kỹ thuật theo yêu cầu của cơ quan có thẩm quyền.

II NỘI DUNG MỚI

NEW

Khẳng định bảo đảm an ninh dữ liệu là bộ phận quan trọng của bảo vệ an ninh mạng

1 Xác lập an ninh dữ liệu là khái niệm pháp lý độc lập, bao gồm bảo đảm chất lượng, tính toàn vẹn và khả năng khai thác dữ liệu.

2 Quản lý toàn bộ vòng đời dữ liệu bằng các biện pháp kỹ thuật, tổ chức và pháp lý như phân quyền, mã hóa, kiểm soát nhân sự và đánh giá rủi ro.

3 Tăng cường kiểm soát dữ liệu xuyên biên giới và bảo vệ cơ sở dữ liệu, trung tâm dữ liệu, hệ thống lưu trữ quan trọng.

4 Nghiêm cấm thu thập, sử dụng, mua bán và phát tán trái phép dữ liệu cá nhân.

5 Tạo cơ sở xử lý vi phạm dữ liệu, phòng chống lừa đảo, mạo danh, chiếm đoạt tài sản và các tội phạm công nghệ cao.

II NỘI DUNG MỚI

NEW

Bổ sung, tăng cường các quy định về bảo vệ trẻ em trên không gian mạng, đồng thời mở rộng yêu cầu bảo vệ đối với người cao tuổi và người có khó khăn trong nhận thức, làm chủ hành vi

Gia đình là tuyến bảo vệ đầu tiên: Cha mẹ, người giám hộ có trách nhiệm quản lý, giám sát việc sử dụng mạng và tài khoản của trẻ em.

Xây dựng mạng lưới bảo vệ đa tầng: Gia đình, doanh nghiệp và cơ quan nhà nước cùng chịu trách nhiệm, hạn chế tình trạng đùn đẩy trách nhiệm.

Doanh nghiệp phải chủ động bảo vệ: Áp dụng biện pháp kỹ thuật để phát hiện, ngăn chặn, gỡ bỏ nội dung xâm hại trẻ em và cung cấp công cụ phản ánh, tố giác thuận tiện.

Mở rộng bảo vệ nhóm yếu thế: Người cao tuổi và người có khó khăn trong nhận thức được cảnh báo sớm, hỗ trợ phù hợp và ưu tiên xử lý các vụ lừa đảo, xâm hại.

II NỘI DUNG MỚI

NEW

Khuyến khích nghiên cứu, phát triển và ứng dụng khoa học, công nghệ trong lĩnh vực an ninh mạng; ưu tiên đầu tư hạ tầng, sản phẩm và dịch vụ an ninh mạng trong nước

1 Phát triển công nghiệp an ninh mạng trong nước thông qua cơ chế đặc biệt ưu đãi đầu tư đối với sản phẩm, dịch vụ và hạ tầng bảo vệ an ninh mạng.

2 Ưu tiên sản phẩm "Make in Vietnam" khi đáp ứng yêu cầu kỹ thuật, chất lượng và an ninh, qua đó tạo thị trường cho doanh nghiệp trong nước.

3 Thúc đẩy nghiên cứu, phát triển và làm chủ công nghệ, hình thành chuỗi giá trị từ R&D, thử nghiệm, chứng nhận đến thương mại hóa.

4 Bảo đảm nguồn lực tài chính, yêu cầu bố trí tối thiểu 15% kinh phí của chương trình, dự án chuyển đổi số và ứng dụng CNTT cho an ninh mạng.

5 Gắn an ninh mạng với thiết kế hệ thống ngay từ đầu, hạn chế tình trạng triển khai xong mới bổ sung bảo mật.

II NHỮNG NỘI DUNG MỚI TRONG LUẬT AN NINH MẠNG NEW

Quy định việc bố trí nguồn lực phù hợp cho bảo đảm an ninh mạng trong các chương trình, đề án, dự án đầu tư chuyển đổi số và ứng dụng công nghệ thông tin

Bố trí tối thiểu 15% tổng kinh phí của chương trình, đề án, dự án chuyển đổi số và ứng dụng CNTT cho bảo vệ an ninh mạng.

Đầu tư toàn diện theo vòng đời dự án, gồm thiết bị, giải pháp bảo mật, dịch vụ giám sát, ứng cứu sự cố và đào tạo nhân lực.

Giảm rủi ro và chi phí khắc phục, hạn chế lộ lọt dữ liệu, gián đoạn dịch vụ và nợ kỹ thuật bảo mật.

Tăng tính minh bạch, kiểm tra và trách nhiệm giải trình của chủ đầu tư, cơ quan quản lý và người đứng đầu.

Bảo đảm chuyển đổi số an toàn, ổn định và bền vững, nâng cao hiệu quả đầu tư công.

II NHỮNG NỘI DUNG MỚI TRONG LUẬT AN NINH MẠNG NEW

Tạo cơ sở pháp lý để mở rộng và tăng cường hợp tác quốc tế về an ninh mạng trên cơ sở tôn trọng độc lập, chủ quyền và lợi ích quốc gia; đồng thời nội luật hóa các nội dung cơ bản của Công ước Liên hợp quốc về phòng, chống tội phạm mạng (Công ước Hà Nội)

1. Hợp tác trên cơ sở tôn trọng chủ quyền, không can thiệp công việc nội bộ, bình đẳng, cùng có lợi và tuân thủ pháp luật Việt Nam.
2. Gắn pháp luật trong nước với điều ước quốc tế, tạo cơ sở cho phối hợp điều tra, thu thập chứng cứ điện tử, bảo toàn dữ liệu và truy vết tội phạm mạng.
3. Thiết lập cơ chế phối hợp thực chất, gồm kênh liên lạc, chia sẻ cảnh báo sớm, trao đổi thông tin, đào tạo và diễn tập.
4. Kiểm soát chặt chẽ việc chia sẻ dữ liệu, nhất là bí mật nhà nước, dữ liệu quan trọng và dữ liệu cá nhân.
5. Nâng cao năng lực và vị thế của Việt Nam, đồng thời bảo đảm lợi ích quốc gia và an ninh quốc gia trong quá trình hội nhập.

CÁC ĐIỀU KIỆN BẢO ĐẢM CHO VIỆC THI HÀNH

III

III CÁC ĐIỀU KIỆN BẢO ĐẢM CHO VIỆC THI HÀNH

Dự kiến nguồn lực để thi hành Luật

Không phát sinh thủ tục hành chính, bộ máy hoặc yêu cầu bổ sung nhân lực.

Các cơ quan, tổ chức thực hiện trong phạm vi chức năng hiện có.

Kinh phí được bảo đảm từ ngân sách trung ương, ngân sách địa phương và các nguồn hợp pháp khác.

Điều kiện bảo đảm cho việc thi hành

Kịp thời ban hành văn bản hướng dẫn và tổ chức chỉ đạo thực hiện.

Tăng cường tuyên truyền, phổ biến pháp luật đến cơ quan, tổ chức và người dân.

Thường xuyên kiểm tra, giám sát việc thi hành Luật và các văn bản hướng dẫn.

TRIỂN KHAI HOẠT ĐỘNG THI HÀNH

IV

IV TRIỂN KHAI HOẠT ĐỘNG THI HÀNH

1. Xây dựng kế hoạch triển khai thi hành Luật.

2. Trình Thủ tướng ban hành danh mục và phân công soạn thảo các nghị định hướng dẫn, tập trung vào bảo vệ hệ thống thông tin, phòng chống tội phạm mạng, biện pháp bảo vệ an ninh mạng, kinh doanh sản phẩm, dịch vụ an ninh mạng, mật mã dân sự và lĩnh vực thuộc Bộ Quốc phòng.

****

3. Xây dựng, ban hành hoặc trình ban hành các văn bản quy định chi tiết, dự kiến trình Chính phủ trong tháng 4/2026.

4. Tổ chức tuyên truyền, phổ biến Luật và các văn bản hướng dẫn thi hành.

Hỏi và Đáp

Luật An ninh mạng năm 2025 được Quốc hội thông qua vào ngày nào và có hiệu lực thi hành từ khi nào?

CÂU TRẢ LỜI

Luật An ninh mạng số 116/2025/QH15 được Quốc hội khóa XV thông qua ngày 10/12/2025 và có hiệu lực thi hành từ ngày **01/7/2026.**

Luật An ninh mạng năm 2025 thay thế những văn bản luật nào ?

CÂU TRẢ LỜI

Kể từ ngày 01/7/2026, Luật An toàn thông tin mạng số 86/2015/QH13, đã được sửa đổi, bổ sung một số điều theo Luật số 35/2018/QH14, và Luật An ninh mạng số 24/2018/QH14 hết hiệu lực thi hành. Luật An ninh mạng năm 2025 kế thừa, hợp nhất các quy định còn phù hợp của hai luật nêu trên, qua đó hình thành khuôn khổ pháp lý thống nhất, đồng bộ về an ninh mạng.

An ninh dữ liệu được hiểu như thế nào theo Luật An ninh mạng năm 2025?

CÂU TRẢ LỜI

An ninh dữ liệu là sự bảo đảm chất lượng dữ liệu và các hoạt động xử lý, sử dụng dữ liệu trên không gian mạng phục vụ phát triển kinh tế - xã hội, chuyển đổi số quốc gia; đồng thời phòng ngừa việc dữ liệu bị truy cập, sử dụng, tiết lộ, sửa đổi trái phép, phá hoại hoặc bị thực hiện hành vi khác đe dọa, gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội.

Hệ thống thông tin được phân loại thành bao nhiêu cấp độ ?

CÂU TRẢ LỜI

Hệ thống thông tin được phân loại thành 05 cấp độ, căn cứ vào mức độ tổn hại có thể xảy ra đối với an ninh quốc gia, trật tự, an toàn xã hội, lợi ích công cộng và quyền, lợi ích hợp pháp của tổ chức, cá nhân khi hệ thống gặp sự cố hoặc có hành vi vi phạm pháp luật về an ninh mạng.

Luật quy định như thế nào đối với hành vi sử dụng trí tuệ nhân tạo hoặc công nghệ mới để giả mạo ?

CÂU TRẢ LỜI

Luật nghiêm cấm hành vi sử dụng trí tuệ nhân tạo hoặc công nghệ mới để giả mạo video, hình ảnh, giọng nói của người khác trái quy định của pháp luật; đồng thời nghiêm cấm việc tạo lập, đăng tải, phát tán các thông tin thuộc nhóm nội dung bị cấm trên không gian mạng. Quy định này là căn cứ pháp lý để phòng ngừa, phát hiện và xử lý các hành vi lợi dụng công nghệ Deepfake và công nghệ mới để lừa đảo, vu khống, xúc phạm danh dự, nhân phẩm hoặc thực hiện hành vi vi phạm pháp luật khác..

Doanh nghiệp cung cấp dịch vụ trên không gian mạng phải thực hiện yêu cầu ngăn chặn, xóa bỏ thông tin vi phạm trong thời hạn bao lâu?

CÂU TRẢ LỜI

Doanh nghiệp trong nước và nước ngoài cung cấp dịch vụ trên mạng viễn thông, mạng Internet và các dịch vụ gia tăng trên không gian mạng tại Việt Nam phải ngăn chặn việc chia sẻ, xóa bỏ thông tin hoặc gỡ bỏ dịch vụ, ứng dụng có nội dung vi phạm chậm nhất là 24 giờ kể từ thời điểm nhận được yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an. Trường hợp khẩn cấp có nguy cơ xâm hại an ninh quốc gia, yêu cầu ngăn chặn, xóa bỏ thông tin phải được thực hiện chậm nhất là 06 giờ..

Trách nhiệm của cha, mẹ hoặc người giám hộ trong việc bảo vệ trẻ em trên không gian mạng được quy định như thế nào ?

CÂU TRẢ LỜI

Trường hợp trẻ em sử dụng dịch vụ giá trị gia tăng trên không gian mạng, cha, mẹ hoặc người giám hộ phải đăng ký tài khoản bằng thông tin của mình; đồng thời có trách nhiệm giám sát, quản lý nội dung mà trẻ em truy cập, đăng tải và chia sẻ trên các nền tảng cung cấp dịch vụ. Cha, mẹ và người giám hộ còn có trách nhiệm bảo đảm quyền của trẻ em và bảo vệ trẻ em khi tham gia không gian mạng theo quy định của pháp luật về trẻ em và pháp luật về an ninh mạng...

Luật quy định như thế nào đối với hành vi mua bán trái pháp luật thông tin, dữ liệu cá nhân ?

CÂU TRẢ LỜI

Luật nghiêm cấm hành vi thu thập, sử dụng, phát tán, trao đổi, chuyển nhượng hoặc kinh doanh trái pháp luật thông tin, dữ liệu cá nhân của người khác. Bên cạnh đó, việc sử dụng danh tính giả, giấy tờ, hồ sơ giả hoặc sử dụng trái phép thông tin của người khác để thành lập doanh nghiệp, đăng ký tài khoản ngân hàng, tài khoản chứng khoán, ví điện tử và các tài khoản số khác; thu thập, trao đổi, mua bán hoặc công khai trái phép thông tin, dữ liệu về các tài khoản này cũng được xác định là hành vi xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng.

Mức kinh phí tối thiểu dành cho bảo vệ an ninh mạng trong các chương trình, đề án, dự án chuyển đổi số và ứng dụng công nghệ thông tin là bao nhiêu?

CÂU TRẢ LỜI

Cơ quan, tổ chức, doanh nghiệp nhà nước, tổ chức chính trị, tổ chức chính trị - xã hội và đơn vị sự nghiệp công lập do ngân sách nhà nước bảo đảm phải bố trí kinh phí bảo vệ an ninh mạng trong dự toán chi hằng năm; đồng thời bố trí tối thiểu 15% tổng kinh phí thực hiện chương trình, đề án, dự án đầu tư chuyển đổi số, ứng dụng công nghệ thông tin để bảo vệ an ninh mạng.

Luật An ninh mạng năm 2025 quy định chuyển tiếp như thế nào?

CÂU TRẢ LỜI

Quy định chuyển tiếp (không có thời hạn 12 tháng chung):

1. Hệ thống thông tin đã xác định cấp độ cũ: Giữ nguyên cấp độ đã xác định, nhưng trong 12 tháng kể từ ngày Luật có hiệu lực phải bảo đảm các điều kiện, tiêu chuẩn và biện pháp bảo vệ an ninh mạng tương ứng theo quy định mới.
2. Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng và mật mã dân sự (cấp trước 01/7/2026): Tiếp tục có giá trị đến hết thời hạn ghi trên giấy phép.
3. Sản phẩm, dịch vụ, giải pháp và phương tiện kỹ thuật bảo đảm an toàn thông tin mạng đã đưa vào sử dụng trước ngày Luật có hiệu lực: Tiếp tục sử dụng, nhưng trong 12 tháng phải bảo đảm điều kiện an ninh mạng theo quy định của Luật.