VĂN BẢN PHÁP LUẬT KHÁC

VĂN BẢN HỢP NHẤT - VĂN PHÒNG QUỐC HỘI

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

LUẬT
AN TOÀN THÔNG TIN MẠNG

Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19 tháng 11 năm 2015 của Quốc hội, có hiệu lực kể từ ngày 01 tháng 7 năm 2016, được sửa đổi, bổ sung bởi:

Luật số 35/2018/QH14 ngày 20 tháng 11 năm 2018 của Quốc hội sửa đổi, bổ sung một số điều của 37 luật có liên quan đến quy hoạch, có hiệu lực kể từ ngày 01 tháng 01 năm 2019.

Căn cứ Hiến pháp nước Cộng hòa xã hội chủ nghĩa Việt Nam;

Quốc hội ban hành Luật An toàn thông tin mạng[1].

---

[1] Luật số 35/2018/QH14 sửa đổi, bổ sung một số điều của 37 luật có liên quan đến quy hoạch có căn cứ ban hành như sau:

"*Căn cứ Hiến pháp nước Cộng hòa xã hội chủ nghĩa Việt Nam;*

Quốc hội ban hành Luật sửa đổi, bổ sung một số điều có liên quan đến quy hoạch của Luật Giao thông đường bộ số 23/2008/QH12, Bộ luật Hàng hải Việt Nam số 95/2015/QH13, Luật Đường sắt số 06/2017/QH14, Luật Giao thông đường thủy nội địa số 23/2004/QH11 đã được sửa đổi, bổ sung một số điều theo Luật số 48/2014/QH13 và Luật số 97/2015/QH13, Luật Tài nguyên nước số 17/2012/QH13 đã được sửa đổi, bổ sung một số điều theo Luật số 08/2017/QH14, Luật Đất đai số 45/2013/QH13, Luật Bảo vệ môi trường số 55/2014/QH13, Luật Khoáng sản số 60/2010/QH12, Luật Khí tượng thủy văn số 90/2015/QH13, Luật Đa dạng sinh học số 20/2008/QH12, Luật Tài nguyên, môi trường biển và hải đảo số 82/2015/QH13, Luật Bảo vệ và kiểm dịch thực vật số 41/2013/QH13, Luật Đê điều số 79/2006/QH11, Luật Thủy lợi số 08/2017/QH14, Luật Năng lượng nguyên tử số 18/2008/QH12, Luật Đo lường số 04/2011/QH13, Luật Tiêu chuẩn và quy chuẩn kỹ thuật số 68/2006/QH11, Luật Chất lượng sản phẩm, hàng hóa số 05/2007/QH12, Luật An toàn thông tin mạng số 86/2015/QH13, Luật Xuất bản số 19/2012/QH13, Luật Báo chí số 103/2016/QH13, Luật Giáo dục quốc phòng và an ninh số 30/2013/QH13, Luật Quản lý, sử dụng vốn nhà nước đầu tư vào sản xuất, kinh doanh tại doanh nghiệp số 69/2014/QH13, Luật Thực hành tiết kiệm, chống lãng phí số 44/2013/QH13 đã được sửa đổi, bổ sung một số điều theo Luật số 21/2017/QH14, Luật Hải quan số 54/2014/QH13 đã được sửa đổi, bổ sung một số điều theo Luật số 71/2014/QH13, Luật Chứng khoán số

Chương I
NHỮNG QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Luật này quy định về hoạt động an toàn thông tin mạng, quyền, trách nhiệm của cơ quan, tổ chức, cá nhân trong việc bảo đảm an toàn thông tin mạng; mật mã dân sự; tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin mạng; kinh doanh trong lĩnh vực an toàn thông tin mạng; phát triển nguồn nhân lực an toàn thông tin mạng; quản lý nhà nước về an toàn thông tin mạng.

Điều 2. Đối tượng áp dụng

Luật này áp dụng đối với cơ quan, tổ chức, cá nhân Việt Nam, tổ chức, cá nhân nước ngoài trực tiếp tham gia hoặc có liên quan đến hoạt động an toàn thông tin mạng tại Việt Nam.

Điều 3. Giải thích từ ngữ

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

1. *An toàn thông tin mạng* là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

2. *Mạng* là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua mạng viễn thông và mạng máy tính.

3. *Hệ thống thông tin* là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên mạng.

4. *Hệ thống thông tin quan trọng quốc gia* là hệ thống thông tin mà khi bị phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới quốc phòng, an ninh quốc gia.

70/2006/QH11 đã được sửa đổi, bổ sung một số điều theo Luật số 62/2010/QH12, Luật Điện ảnh số 62/2006/QH11 đã được sửa đổi, bổ sung một số điều theo Luật số 31/2009/QH12, Luật Quảng cáo số 16/2012/QH13, Luật Xây dựng số 50/2014/QH13 đã được sửa đổi, bổ sung một số điều theo Luật số 03/2016/QH14, Luật Quy hoạch đô thị số 30/2009/QH12 đã được sửa đổi, bổ sung một số điều theo Luật số 77/2015/QH13, Luật Dầu khí năm 1993 đã được sửa đổi, bổ sung một số điều theo Luật số 19/2000/QH10 và Luật số 10/2008/QH12, Bộ luật Lao động số 10/2012/QH13 đã được sửa đổi, bổ sung một số điều theo Luật số 92/2015/QH13, Luật Bảo hiểm xã hội số 58/2014/QH13, Luật Bảo hiểm y tế số 25/2008/QH12 đã được sửa đổi, bổ sung một số điều theo Luật số 32/2013/QH13, Luật số 46/2014/QH13 và Luật số 97/2015/QH13, Luật Phòng, chống bệnh truyền nhiễm số 03/2007/QH12, Luật Giám định tư pháp số 13/2012/QH13 và Luật Bảo vệ quyền lợi người tiêu dùng số 59/2010/QH12.”

5. *Chủ quản hệ thống thông tin* là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin.

6. *Xâm phạm an toàn thông tin mạng* là hành vi truy nhập, sử dụng, tiết lộ, làm gián đoạn, sửa đổi, phá hoại trái phép thông tin, hệ thống thông tin.

7. *Sự cố an toàn thông tin mạng* là việc thông tin, hệ thống thông tin bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.

8. *Rủi ro an toàn thông tin mạng* là những nhân tố chủ quan hoặc khách quan có khả năng ảnh hưởng tới trạng thái an toàn thông tin mạng.

9. *Đánh giá rủi ro an toàn thông tin mạng* là việc phát hiện, phân tích, ước lượng mức độ tổn hại, mối đe dọa đối với thông tin, hệ thống thông tin.

10. *Quản lý rủi ro an toàn thông tin mạng* là việc đưa ra các biện pháp nhằm giảm thiểu rủi ro an toàn thông tin mạng.

11. *Phần mềm độc hại* là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

12. *Hệ thống lọc phần mềm độc hại* là tập hợp phần cứng, phần mềm được kết nối vào mạng để phát hiện, ngăn chặn, lọc và thống kê phần mềm độc hại.

13. *Địa chỉ điện tử* là địa chỉ được sử dụng để gửi, nhận thông tin trên mạng bao gồm địa chỉ thư điện tử, số điện thoại, địa chỉ Internet và hình thức tương tự khác.

14. *Xung đột thông tin* là việc hai hoặc nhiều tổ chức trong nước và nước ngoài sử dụng biện pháp công nghệ, kỹ thuật thông tin gây tổn hại đến thông tin, hệ thống thông tin trên mạng.

15. *Thông tin cá nhân* là thông tin gắn với việc xác định danh tính của một người cụ thể.

16. *Chủ thể thông tin cá nhân* là người được xác định từ thông tin cá nhân đó.

17. *Xử lý thông tin cá nhân* là việc thực hiện một hoặc một số thao tác thu thập, biên tập, sử dụng, lưu trữ, cung cấp, chia sẻ, phát tán thông tin cá nhân trên mạng nhằm mục đích thương mại.

18. *Mật mã dân sự* là kỹ thuật mật mã và sản phẩm mật mã được sử dụng để bảo mật hoặc xác thực đối với thông tin không thuộc phạm vi bí mật nhà nước.

19. *Sản phẩm an toàn thông tin mạng* là phần cứng, phần mềm có chức năng bảo vệ thông tin, hệ thống thông tin.

20. *Dịch vụ an toàn thông tin mạng* là dịch vụ bảo vệ thông tin, hệ thống thông tin.

Điều 4. Nguyên tắc bảo đảm an toàn thông tin mạng

1. Cơ quan, tổ chức, cá nhân có trách nhiệm bảo đảm an toàn thông tin mạng. Hoạt động an toàn thông tin mạng của cơ quan, tổ chức, cá nhân phải đúng quy định của pháp luật, bảo đảm quốc phòng, an ninh quốc gia, bí mật nhà nước, giữ vững ổn định chính trị, trật tự, an toàn xã hội và thúc đẩy phát triển kinh tế - xã hội.

2. Tổ chức, cá nhân không được xâm phạm an toàn thông tin mạng của tổ chức, cá nhân khác.

3. Việc xử lý sự cố an toàn thông tin mạng phải bảo đảm quyền và lợi ích hợp pháp của tổ chức, cá nhân, không xâm phạm đến đời sống riêng tư, bí mật cá nhân, bí mật gia đình của cá nhân, thông tin riêng của tổ chức.

4. Hoạt động an toàn thông tin mạng phải được thực hiện thường xuyên, liên tục, kịp thời và hiệu quả.

Điều 5. Chính sách của Nhà nước về an toàn thông tin mạng

1. Đẩy mạnh đào tạo, phát triển nguồn nhân lực và xây dựng cơ sở hạ tầng, kỹ thuật an toàn thông tin mạng đáp ứng yêu cầu ổn định chính trị, phát triển kinh tế - xã hội, bảo đảm quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội.

2. Khuyến khích nghiên cứu, phát triển, áp dụng biện pháp kỹ thuật, công nghệ, hỗ trợ xuất khẩu, mở rộng thị trường cho sản phẩm, dịch vụ an toàn thông tin mạng do tổ chức, cá nhân trong nước sản xuất, cung cấp; tạo điều kiện nhập khẩu sản phẩm, công nghệ hiện đại mà tổ chức, cá nhân trong nước chưa có năng lực sản xuất, cung cấp.

3. Bảo đảm môi trường cạnh tranh lành mạnh trong hoạt động kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng; khuyến khích, tạo điều kiện cho tổ chức, cá nhân tham gia đầu tư, nghiên cứu, phát triển và cung cấp sản phẩm, dịch vụ an toàn thông tin mạng.

4. Nhà nước bố trí kinh phí để bảo đảm an toàn thông tin mạng của cơ quan nhà nước và an toàn thông tin mạng cho hệ thống thông tin quan trọng quốc gia.

Điều 6. Hợp tác quốc tế về an toàn thông tin mạng

1. Hợp tác quốc tế về an toàn thông tin mạng phải tuân thủ các nguyên tắc sau đây:

a) Tôn trọng độc lập, chủ quyền và toàn vẹn lãnh thổ quốc gia, không can thiệp vào công việc nội bộ của nhau, bình đẳng và các bên cùng có lợi;

b) Phù hợp với quy định của pháp luật Việt Nam, điều ước quốc tế mà Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên.

2. Nội dung hợp tác quốc tế về an toàn thông tin mạng gồm:

a) Hợp tác quốc tế trong đào tạo, nghiên cứu và ứng dụng khoa học, kỹ thuật, công nghệ về an toàn thông tin mạng;

b) Hợp tác quốc tế trong phòng, chống hành vi vi phạm pháp luật về an toàn thông tin mạng; điều tra, xử lý sự cố an toàn thông tin mạng, ngăn chặn hoạt động lợi dụng mạng để khủng bố;

c) Hoạt động hợp tác quốc tế khác về an toàn thông tin mạng.

Điều 7. Các hành vi bị nghiêm cấm

1. Ngăn chặn việc truyền tải thông tin trên mạng, can thiệp, truy nhập, gây nguy hại, xóa, thay đổi, sao chép và làm sai lệch thông tin trên mạng trái pháp luật.

2. Gây ảnh hưởng, cản trở trái pháp luật tới hoạt động bình thường của hệ thống thông tin hoặc tới khả năng truy nhập hệ thống thông tin của người sử dụng.

3. Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của biện pháp bảo vệ an toàn thông tin mạng của hệ thống thông tin; tấn công, chiếm quyền điều khiển, phá hoại hệ thống thông tin.

4. Phát tán thư rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo.

5. Thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác; lợi dụng sơ hở, điểm yếu của hệ thống thông tin để thu thập, khai thác thông tin cá nhân.

6. Xâm nhập trái pháp luật bí mật mật mã và thông tin đã mã hóa hợp pháp của cơ quan, tổ chức, cá nhân; tiết lộ thông tin về sản phẩm mật mã dân sự, thông tin về khách hàng sử dụng hợp pháp sản phẩm mật mã dân sự; sử dụng, kinh doanh các sản phẩm mật mã dân sự không rõ nguồn gốc.

Điều 8. Xử lý vi phạm pháp luật về an toàn thông tin mạng

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 phạt 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.

Chương II
BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Mục 1
BẢO VỆ THÔNG TIN MẠNG

Điều 9. Phân loại thông tin

1. Cơ quan, tổ chức sở hữu thông tin phân loại thông tin theo thuộc tính bí mật để có biện pháp bảo vệ phù hợp.

2. Thông tin thuộc phạm vi bí mật nhà nước được phân loại và bảo vệ theo quy định của pháp luật về bảo vệ bí mật nhà nước.

Cơ quan, tổ chức sử dụng thông tin đã phân loại và chưa phân loại trong hoạt động thuộc lĩnh vực của mình phải có trách nhiệm xây dựng quy định, thủ tục để xử lý thông tin; xác định nội dung và phương pháp ghi truy nhập được phép vào thông tin đã được phân loại.

Điều 10. Quản lý gửi thông tin

1. Việc gửi thông tin trên mạng phải bảo đảm các yêu cầu sau đây:

a) Không giả mạo nguồn gốc gửi thông tin;

b) Tuân thủ quy định của Luật này và quy định khác của pháp luật có liên quan.

2. Tổ chức, cá nhân không được gửi thông tin mang tính thương mại vào địa chỉ điện tử của người tiếp nhận khi chưa được người tiếp nhận đồng ý hoặc khi người tiếp nhận đã từ chối, trừ trường hợp người tiếp nhận có nghĩa vụ phải tiếp nhận thông tin theo quy định của pháp luật.

3. Doanh nghiệp viễn thông, doanh nghiệp cung cấp dịch vụ ứng dụng viễn thông và doanh nghiệp cung cấp dịch vụ công nghệ thông tin gửi thông tin có trách nhiệm sau đây:

a) Tuân thủ quy định của pháp luật về lưu trữ thông tin, bảo vệ thông tin cá nhân, thông tin riêng của tổ chức, cá nhân;

b) Áp dụng biện pháp ngăn chặn, xử lý khi nhận được thông báo của tổ chức, cá nhân về việc gửi thông tin vi phạm quy định của pháp luật;

c) Có phương thức để người tiếp nhận thông tin có khả năng từ chối việc tiếp nhận thông tin;

d) Cung cấp điều kiện kỹ thuật và nghiệp vụ cần thiết để cơ quan nhà nước có thẩm quyền thực hiện nhiệm vụ quản lý, bảo đảm an toàn thông tin mạng khi có yêu cầu.

Điều 11. Phòng ngừa, phát hiện, ngăn chặn và xử lý phần mềm độc hại

1. Cơ quan, tổ chức, cá nhân có trách nhiệm thực hiện phòng ngừa, ngăn chặn phần mềm độc hại theo hướng dẫn, yêu cầu của cơ quan nhà nước có thẩm quyền.

2. Chủ quản hệ thống thông tin quan trọng quốc gia triển khai hệ thống kỹ thuật nghiệp vụ nhằm phòng ngừa, phát hiện, ngăn chặn và xử lý kịp thời phần mềm độc hại.

3. Doanh nghiệp cung cấp dịch vụ thư điện tử, truyền đưa, lưu trữ thông tin phải có hệ thống lọc phần mềm độc hại trong quá trình gửi, nhận, lưu trữ thông tin trên hệ thống của mình và báo cáo cơ quan nhà nước có thẩm quyền theo quy định của pháp luật.

4. Doanh nghiệp cung cấp dịch vụ Internet có biện pháp quản lý, phòng ngừa, phát hiện, ngăn chặn phát tán phần mềm độc hại và xử lý theo yêu cầu của cơ quan nhà nước có thẩm quyền.

5. Bộ Thông tin và Truyền thông chủ trì, phối hợp với Bộ Quốc phòng, Bộ Công an và bộ, ngành có liên quan tổ chức phòng ngừa, phát hiện, ngăn chặn và xử lý phần mềm độc hại gây ảnh hưởng đến quốc phòng, an ninh quốc gia.

Điều 12. Bảo đảm an toàn tài nguyên viễn thông

1. Cơ quan, tổ chức, cá nhân sử dụng tài nguyên viễn thông có trách nhiệm sau đây:

a) Áp dụng biện pháp quản lý và kỹ thuật để ngăn chặn mất an toàn thông tin mạng xuất phát từ tần số, kho số, tên miền và địa chỉ Internet của mình;

b) Phối hợp, cung cấp thông tin liên quan đến an toàn tài nguyên viễn thông theo yêu cầu của cơ quan nhà nước có thẩm quyền.

2. Doanh nghiệp cung cấp dịch vụ trên Internet có trách nhiệm quản lý, phối hợp ngăn chặn mất an toàn thông tin mạng xuất phát từ tài nguyên Internet, từ khách hàng của mình; cung cấp đầy đủ thông tin theo yêu cầu của cơ quan nhà nước có thẩm quyền; phối hợp kết nối, định tuyến để bảo đảm hệ thống máy chủ tên miền quốc gia Việt Nam hoạt động an toàn, ổn định.

3. Bộ Thông tin và Truyền thông có trách nhiệm thực hiện bảo đảm an toàn thông tin mạng cho hệ thống máy chủ tên miền quốc gia Việt Nam.

Điều 13. Ứng cứu sự cố an toàn thông tin mạng

1. Ứng cứu sự cố an toàn thông tin mạng là hoạt động nhằm xử lý, khắc phục sự cố gây mất an toàn thông tin mạng.

2. Ứng cứu sự cố an toàn thông tin mạng phải tuân thủ các nguyên tắc sau đây:

a) Kịp thời, nhanh chóng, chính xác, đồng bộ và hiệu quả;

b) Tuân thủ quy định của pháp luật về điều phối ứng cứu sự cố an toàn thông tin mạng;

c) Có sự phối hợp giữa cơ quan, tổ chức, doanh nghiệp trong nước và nước ngoài.

3. Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân cấp tỉnh, doanh nghiệp viễn thông, chủ quản hệ thống thông tin quan trọng quốc gia phải thành lập hoặc chỉ định bộ phận chuyên trách ứng cứu sự cố an toàn thông tin mạng.

4. Bộ Thông tin và Truyền thông có trách nhiệm điều phối ứng cứu sự cố an toàn thông tin mạng trên toàn quốc; quy định chi tiết về điều phối ứng cứu sự cố an toàn thông tin mạng.

Điều 14. Ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia

1. Ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia là hoạt động ứng cứu sự cố trong tình huống thảm họa hoặc theo yêu cầu của cơ quan nhà nước có thẩm quyền nhằm bảo đảm an toàn thông tin mạng quốc gia.

2. Ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia phải tuân thủ các nguyên tắc sau đây:

a) Tổ chức thực hiện theo phân cấp;

b) Thực hiện tại chỗ, nhanh chóng, nghiêm ngặt, phối hợp chặt chẽ;

c) Áp dụng các biện pháp kỹ thuật, bảo đảm hiệu quả, khả thi.

3. Hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia gồm:

a) Phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

b) Phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng của cơ quan nhà nước, tổ chức chính trị, tổ chức chính trị - xã hội;

c) Phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng của địa phương;

d) Phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng của doanh nghiệp viễn thông.

4. Trách nhiệm bảo đảm an toàn thông tin mạng quốc gia được quy định như sau:

a) Thủ tướng Chính phủ quyết định hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

b) Bộ Thông tin và Truyền thông có trách nhiệm chủ trì điều phối công tác ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

c) Bộ, ngành, Ủy ban nhân dân các cấp và cơ quan, tổ chức có liên quan trong phạm vi nhiệm vụ, quyền hạn của mình có trách nhiệm phối hợp, chỉ đạo ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

d) Doanh nghiệp viễn thông có trách nhiệm thực hiện biện pháp ứng cứu khẩn cấp, phối hợp với Bộ Thông tin và Truyền thông, bộ, ngành, Ủy ban nhân dân các cấp có liên quan để bảo đảm an toàn thông tin mạng quốc gia.

Điều 15. Trách nhiệm của cơ quan, tổ chức, cá nhân trong bảo đảm an toàn thông tin mạng

1. Cơ quan, tổ chức, cá nhân tham gia hoạt động an toàn thông tin mạng có trách nhiệm phối hợp với cơ quan nhà nước có thẩm quyền và tổ chức, cá nhân khác trong việc bảo đảm an toàn thông tin mạng.

2. Cơ quan, tổ chức, cá nhân sử dụng dịch vụ trên mạng có trách nhiệm thông báo kịp thời cho doanh nghiệp cung cấp dịch vụ hoặc bộ phận chuyên trách ứng cứu sự cố khi phát hiện các hành vi phá hoại hoặc sự cố an toàn thông tin mạng.

Mục 2
BẢO VỆ THÔNG TIN CÁ NHÂN

Điều 16. Nguyên tắc bảo vệ thông tin cá nhân trên mạng

1. Cá nhân tự bảo vệ thông tin cá nhân của mình và tuân thủ quy định của pháp luật về cung cấp thông tin cá nhân khi sử dụng dịch vụ trên mạng.

2. Cơ quan, tổ chức, cá nhân xử lý thông tin cá nhân có trách nhiệm bảo đảm an toàn thông tin mạng đối với thông tin do mình xử lý.

3. Tổ chức, cá nhân xử lý thông tin cá nhân phải xây dựng và công bố công khai biện pháp xử lý, bảo vệ thông tin cá nhân của tổ chức, cá nhân mình.

4. Việc bảo vệ thông tin cá nhân thực hiện theo quy định của Luật này và quy định khác của pháp luật có liên quan.

5. Việc xử lý thông tin cá nhân phục vụ mục đích bảo đảm quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội hoặc không nhằm mục đích thương mại được thực hiện theo quy định khác của pháp luật có liên quan.

Điều 17. Thu thập và sử dụng thông tin cá nhân

1. Tổ chức, cá nhân xử lý thông tin cá nhân có trách nhiệm sau đây:

a) Tiến hành thu thập thông tin cá nhân sau khi có sự đồng ý của chủ thể thông tin cá nhân về phạm vi, mục đích của việc thu thập và sử dụng thông tin đó;

b) Chỉ sử dụng thông tin cá nhân đã thu thập vào mục đích khác mục đích ban đầu sau khi có sự đồng ý của chủ thể thông tin cá nhân;

c) Không được cung cấp, chia sẻ, phát tán thông tin cá nhân mà mình đã thu thập, tiếp cận, kiểm soát cho bên thứ ba, trừ trường hợp có sự đồng ý của chủ thể thông tin cá nhân đó hoặc theo yêu cầu của cơ quan nhà nước có thẩm quyền.

2. Cơ quan nhà nước chịu trách nhiệm bảo mật, lưu trữ thông tin cá nhân do mình thu thập.

3. Chủ thể thông tin cá nhân có quyền yêu cầu tổ chức, cá nhân xử lý thông tin cá nhân cung cấp thông tin cá nhân của mình mà tổ chức, cá nhân đó đã thu thập, lưu trữ.

Điều 18. Cập nhật, sửa đổi và hủy bỏ thông tin cá nhân

1. Chủ thể thông tin cá nhân có quyền yêu cầu tổ chức, cá nhân xử lý thông tin cá nhân cập nhật, sửa đổi, hủy bỏ thông tin cá nhân của mình mà tổ chức, cá nhân đó đã thu thập, lưu trữ hoặc ngừng cung cấp thông tin cá nhân của mình cho bên thứ ba.

2. Ngay khi nhận được yêu cầu của chủ thể thông tin cá nhân về việc cập nhật, sửa đổi, hủy bỏ thông tin cá nhân hoặc đề nghị ngừng cung cấp thông tin cá nhân cho bên thứ ba, tổ chức, cá nhân xử lý thông tin cá nhân có trách nhiệm sau đây:

a) Thực hiện yêu cầu và thông báo cho chủ thể thông tin cá nhân hoặc cung cấp cho chủ thể thông tin cá nhân quyền tiếp cận để tự cập nhật, sửa đổi, hủy bỏ thông tin cá nhân của mình;

b) Áp dụng biện pháp phù hợp để bảo vệ thông tin cá nhân; thông báo cho chủ thể thông tin cá nhân đó trong trường hợp chưa thực hiện được yêu cầu do yếu tố kỹ thuật hoặc yếu tố khác.

3. Tổ chức, cá nhân xử lý thông tin cá nhân phải hủy bỏ thông tin cá nhân đã được lưu trữ khi đã hoàn thành mục đích sử dụng hoặc hết thời hạn lưu trữ và thông báo cho chủ thể thông tin cá nhân biết, trừ trường hợp pháp luật có quy định khác.

Điều 19. Bảo đảm an toàn thông tin cá nhân trên mạng

1. Tổ chức, cá nhân xử lý thông tin cá nhân phải áp dụng biện pháp quản lý, kỹ thuật phù hợp để bảo vệ thông tin cá nhân do mình thu thập, lưu trữ; tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật về bảo đảm an toàn thông tin mạng.

2. Khi xảy ra hoặc có nguy cơ xảy ra sự cố an toàn thông tin mạng, tổ chức, cá nhân xử lý thông tin cá nhân cần áp dụng biện pháp khắc phục, ngăn chặn trong thời gian sớm nhất.

Điều 20. Trách nhiệm của cơ quan quản lý nhà nước trong bảo vệ thông tin cá nhân trên mạng

1. Thiết lập kênh thông tin trực tuyến để tiếp nhận kiến nghị, phản ánh của tổ chức, cá nhân liên quan đến bảo đảm an toàn thông tin cá nhân trên mạng.

2. Định kỳ hằng năm tổ chức thanh tra, kiểm tra đối với tổ chức, cá nhân xử lý thông tin cá nhân; tổ chức thanh tra, kiểm tra đột xuất trong trường hợp cần thiết.

Mục 3
BẢO VỆ HỆ THỐNG THÔNG TIN

Điều 21. Phân loại cấp độ an toàn hệ thống thông tin

1. Phân loại cấp độ an toàn hệ thống thông tin là việc xác định cấp độ an toàn thông tin của hệ thống thông tin theo cấp độ tăng dần từ 1 đến 5 để áp dụng biện pháp quản lý và kỹ thuật nhằm bảo vệ hệ thống thông tin phù hợp theo cấp độ.

2. Hệ thống thông tin được phân loại theo cấp độ an toàn như sau:

a) Cấp độ 1 là cấp độ mà khi bị phá hoại sẽ làm tổn hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân nhưng không làm tổn hại tới lợi ích công cộng, trật tự, an toàn xã hội, quốc phòng, an ninh quốc gia;

b) Cấp độ 2 là cấp độ mà khi bị phá hoại sẽ làm tổn hại nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc làm tổn hại tới lợi ích công cộng nhưng không làm tổn hại tới trật tự, an toàn xã hội, quốc phòng, an ninh quốc gia;

c) Cấp độ 3 là cấp độ mà khi bị phá hoại sẽ làm tổn hại nghiêm trọng tới sản xuất, lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại tới quốc phòng, an ninh quốc gia;

d) Cấp độ 4 là cấp độ mà khi bị phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại nghiêm trọng tới quốc phòng, an ninh quốc gia;

đ) Cấp độ 5 là cấp độ mà khi bị phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới quốc phòng, an ninh quốc gia.

3. Chính phủ quy định chi tiết về tiêu chí, thẩm quyền, trình tự, thủ tục xác định cấp độ an toàn hệ thống thông tin và trách nhiệm bảo đảm an toàn hệ thống thông tin theo từng cấp độ.

Điều 22. Nhiệm vụ bảo vệ hệ thống thông tin

1. Xác định cấp độ an toàn thông tin của hệ thống thông tin.

2. Đánh giá và quản lý rủi ro an toàn hệ thống thông tin.

3. Đôn đốc, giám sát, kiểm tra công tác bảo vệ hệ thống thông tin.

4. Tổ chức triển khai các biện pháp bảo vệ hệ thống thông tin.

5. Thực hiện chế độ báo cáo theo quy định.

6. Tổ chức tuyên truyền, nâng cao nhận thức về an toàn thông tin mạng.

Điều 23. Biện pháp bảo vệ hệ thống thông tin

1. Ban hành quy định về bảo đảm an toàn thông tin mạng trong thiết kế, xây dựng, quản lý, vận hành, sử dụng, nâng cấp, hủy bỏ hệ thống thông tin.

2. Áp dụng biện pháp quản lý, kỹ thuật theo tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin mạng để phòng, chống nguy cơ, khắc phục sự cố an toàn thông tin mạng.

3. Kiểm tra, giám sát việc tuân thủ quy định và đánh giá hiệu quả của các biện pháp quản lý và kỹ thuật được áp dụng.

4. Giám sát an toàn hệ thống thông tin.

Điều 24. Giám sát an toàn hệ thống thông tin

1. Giám sát an toàn hệ thống thông tin là hoạt động lựa chọn đối tượng giám sát, thu thập, phân tích trạng thái thông tin của đối tượng giám sát nhằm xác định những nhân tố ảnh hưởng đến an toàn hệ thống thông tin; báo cáo, cảnh báo hành vi xâm phạm an toàn thông tin mạng hoặc hành vi có khả năng gây ra sự cố an toàn thông tin mạng đối với hệ thống thông tin; tiến hành phân tích yếu tố then chốt ảnh hưởng tới trạng thái an toàn thông tin mạng; đề xuất thay đổi biện pháp kỹ thuật.

2. Đối tượng giám sát an toàn hệ thống thông tin gồm tường lửa, kiểm soát truy nhập, tuyến thông tin chủ yếu, máy chủ quan trọng, thiết bị quan trọng hoặc thiết bị đầu cuối quan trọng.

3. Doanh nghiệp viễn thông, doanh nghiệp cung cấp dịch vụ công nghệ thông tin, doanh nghiệp cung cấp dịch vụ an toàn thông tin mạng có trách nhiệm phối hợp với chủ quản hệ thống thông tin trong việc giám sát an toàn hệ thống thông tin theo yêu cầu của cơ quan nhà nước có thẩm quyền.

Điều 25. Trách nhiệm của chủ quản hệ thống thông tin

1. Chủ quản hệ thống thông tin có trách nhiệm thực hiện bảo vệ hệ thống thông tin theo quy định tại các điều 22, 23 và 24 của Luật này.

2. Chủ quản hệ thống thông tin sử dụng ngân sách nhà nước thực hiện trách nhiệm quy định tại khoản 1 Điều này và có trách nhiệm sau đây:

a) Có phương án bảo đảm an toàn thông tin mạng được cơ quan nhà nước có thẩm quyền thẩm định khi thiết lập, mở rộng hoặc nâng cấp hệ thống thông tin;

b) Chỉ định cá nhân, bộ phận phụ trách về an toàn thông tin mạng.

Điều 26. Hệ thống thông tin quan trọng quốc gia

1. Khi thiết lập, mở rộng và nâng cấp hệ thống thông tin quan trọng quốc gia phải thực hiện kiểm định an toàn thông tin trước khi đưa vào vận hành, khai thác.

2. Bộ Thông tin và Truyền thông chủ trì, phối hợp với Bộ Quốc phòng, Bộ Công an và bộ, ngành có liên quan xây dựng Danh mục hệ thống thông tin quan trọng quốc gia trình Thủ tướng Chính phủ ban hành.

Điều 27. Trách nhiệm bảo đảm an toàn thông tin mạng cho hệ thống thông tin quan trọng quốc gia

1. Chủ quản hệ thống thông tin quan trọng quốc gia có trách nhiệm sau đây:

a) Thực hiện quy định tại khoản 2 Điều 25 của Luật này;

b) Định kỳ đánh giá rủi ro an toàn thông tin mạng. Việc đánh giá rủi ro an toàn thông tin mạng phải do tổ chức chuyên môn được cơ quan nhà nước có thẩm quyền chỉ định thực hiện;

c) Triển khai biện pháp dự phòng cho hệ thống thông tin;

d) Lập kế hoạch bảo vệ, lập phương án và diễn tập phương án bảo vệ hệ thống thông tin quan trọng quốc gia.

2. Bộ Thông tin và Truyền thông có trách nhiệm sau đây:

a) Chủ trì, phối hợp với chủ quản hệ thống thông tin quan trọng quốc gia, Bộ Công an và bộ, ngành có liên quan hướng dẫn, đôn đốc, thanh tra, kiểm tra công tác bảo vệ an toàn thông tin mạng đối với hệ thống thông tin quan trọng quốc gia, trừ hệ thống thông tin quy định tại khoản 3 và khoản 4 Điều này;

b) Yêu cầu doanh nghiệp viễn thông, doanh nghiệp cung cấp dịch vụ công nghệ thông tin, doanh nghiệp cung cấp dịch vụ an toàn thông tin mạng tham gia tư vấn, hỗ trợ kỹ thuật, ứng cứu sự cố an toàn thông tin mạng cho hệ thống thông tin quan trọng quốc gia.

3. Bộ Công an chủ trì hướng dẫn, đôn đốc, thanh tra, kiểm tra công tác bảo vệ an toàn thông tin mạng đối với hệ thống thông tin quan trọng quốc gia do Bộ Công an quản lý; phối hợp với Bộ Thông tin và Truyền thông, chủ quản hệ thống thông tin quan trọng quốc gia, bộ, ngành, Ủy ban nhân dân các cấp có liên quan trong việc bảo vệ hệ thống thông tin quan trọng quốc gia khác khi có yêu cầu của cơ quan nhà nước có thẩm quyền.

4. Bộ Quốc phòng chủ trì hướng dẫn, đôn đốc, thanh tra, kiểm tra công tác bảo vệ an toàn thông tin mạng đối với hệ thống thông tin quan trọng quốc gia do Bộ Quốc phòng quản lý.

5. Ban Cơ yếu Chính phủ chủ trì tổ chức triển khai giải pháp dùng mật mã để bảo vệ thông tin trong hệ thống thông tin quan trọng quốc gia của cơ quan nhà nước, tổ chức chính trị, tổ chức chính trị - xã hội; phối hợp với chủ quản hệ thống thông tin quan trọng quốc gia trong việc giám sát an toàn thông tin mạng theo quy định của pháp luật.

Mục 4
NGĂN CHẶN XUNG ĐỘT THÔNG TIN TRÊN MẠNG

Điều 28. Trách nhiệm của tổ chức, cá nhân trong việc ngăn chặn xung đột thông tin trên mạng

1. Tổ chức, cá nhân trong phạm vi nhiệm vụ, quyền hạn của mình có trách nhiệm sau đây:

a) Ngăn chặn thông tin phá hoại xuất phát từ hệ thống thông tin của mình; hợp tác xác định nguồn, đẩy lùi, khắc phục hậu quả tấn công mạng được thực hiện thông qua hệ thống thông tin của tổ chức, cá nhân trong nước và nước ngoài;

b) Ngăn chặn hành động của tổ chức, cá nhân trong nước và nước ngoài có mục đích phá hoại tính nguyên vẹn của mạng;

c) Loại trừ việc tổ chức thực hiện hoạt động trái pháp luật trên mạng có ảnh hưởng nghiêm trọng đến quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội của tổ chức, cá nhân trong nước và nước ngoài.

2. Chính phủ quy định chi tiết về ngăn chặn xung đột thông tin trên mạng.

Điều 29. Ngăn chặn hoạt động sử dụng mạng để khủng bố

1. Các biện pháp ngăn chặn hoạt động sử dụng mạng để khủng bố gồm:

a) Vô hiệu hóa nguồn Internet sử dụng để thực hiện hành vi khủng bố;

b) Ngăn chặn việc thiết lập và mở rộng trao đổi thông tin về các tín hiệu, nhân tố, phương pháp và cách sử dụng Internet để thực hiện hành vi khủng bố, về mục tiêu và hoạt động của các tổ chức khủng bố trên mạng;

c) Trao đổi kinh nghiệm và thực tiễn kiểm soát các nguồn Internet, tìm và kiểm soát nội dung của trang tin điện tử có mục đích khủng bố.

2. Chính phủ quy định chi tiết về trách nhiệm thực hiện và các biện pháp ngăn chặn hoạt động sử dụng mạng để khủng bố quy định tại khoản 1 Điều này.

Chương III
MẬT MÃ DÂN SỰ

Điều 30. Sản phẩm, dịch vụ mật mã dân sự

1. Sản phẩm mật mã dân sự là các tài liệu, trang thiết bị kỹ thuật và nghiệp vụ mật mã để bảo vệ thông tin không thuộc phạm vi bí mật nhà nước.

2. Dịch vụ mật mã dân sự gồm dịch vụ bảo vệ thông tin sử dụng sản phẩm mật mã dân sự; kiểm định, đánh giá sản phẩm mật mã dân sự; tư vấn bảo mật, an toàn thông tin mạng sử dụng sản phẩm mật mã dân sự.

Điều 31. Kinh doanh sản phẩm, dịch vụ mật mã dân sự

1. Doanh nghiệp phải có Giấy phép kinh doanh sản phẩm, dịch vụ mật mã dân sự khi kinh doanh sản phẩm, dịch vụ mật mã dân sự thuộc Danh mục sản phẩm, dịch vụ mật mã dân sự.

2. Doanh nghiệp được cấp Giấy phép kinh doanh sản phẩm, dịch vụ mật mã dân sự khi đáp ứng đủ các điều kiện sau đây:

a) Có đội ngũ quản lý, điều hành, kỹ thuật đáp ứng yêu cầu chuyên môn về bảo mật, an toàn thông tin;

b) Có hệ thống trang thiết bị, cơ sở vật chất phù hợp với quy mô cung cấp sản phẩm, dịch vụ mật mã dân sự;

c) Có phương án kỹ thuật phù hợp với tiêu chuẩn, quy chuẩn kỹ thuật;

d) Có phương án bảo mật và an toàn thông tin mạng trong quá trình quản lý và cung cấp sản phẩm, dịch vụ mật mã dân sự;

đ) Có phương án kinh doanh phù hợp.

3. Sản phẩm mật mã dân sự phải được kiểm định, chứng nhận hợp quy trước khi lưu thông trên thị trường.

4. Doanh nghiệp được cấp Giấy phép kinh doanh sản phẩm, dịch vụ mật mã dân sự phải nộp phí theo quy định của pháp luật về phí và lệ phí.

5. Chính phủ ban hành Danh mục sản phẩm, dịch vụ mật mã dân sự và quy định chi tiết Điều này.

Điều 32. Trình tự, thủ tục đề nghị cấp Giấy phép kinh doanh sản phẩm, dịch vụ mật mã dân sự

1. Doanh nghiệp đề nghị cấp Giấy phép kinh doanh sản phẩm, dịch vụ mật mã dân sự nộp hồ sơ đề nghị cấp Giấy phép tại Ban Cơ yếu Chính phủ.

2. Hồ sơ đề nghị cấp Giấy phép kinh doanh sản phẩm, dịch vụ mật mã dân sự được lập thành hai bộ, gồm:

a) Đơn đề nghị cấp Giấy phép kinh doanh sản phẩm, dịch vụ mật mã dân sự;

b) Bản sao Giấy chứng nhận đăng ký doanh nghiệp hoặc Giấy chứng nhận đăng ký đầu tư hoặc giấy tờ khác có giá trị tương đương;

c) Bản sao văn bằng hoặc chứng chỉ chuyên môn về bảo mật, an toàn thông tin của đội ngũ quản lý, điều hành, kỹ thuật;

d) Phương án kỹ thuật gồm tài liệu về đặc tính kỹ thuật, tham số kỹ thuật của sản phẩm; tiêu chuẩn, quy chuẩn kỹ thuật của sản phẩm; tiêu chuẩn, chất lượng dịch vụ; các biện pháp, giải pháp kỹ thuật; phương án bảo hành, bảo trì sản phẩm;

đ) Phương án bảo mật và an toàn thông tin mạng trong quá trình quản lý và cung cấp sản phẩm, dịch vụ mật mã dân sự;

e) Phương án kinh doanh gồm phạm vi, đối tượng cung cấp, quy mô số lượng sản phẩm, dịch vụ hệ thống phục vụ khách hàng và bảo đảm kỹ thuật.

3. Trong thời hạn 30 ngày kể từ ngày nhận đủ hồ sơ, Ban Cơ yếu Chính phủ thẩm định và cấp Giấy phép kinh doanh sản phẩm, dịch vụ mật mã dân sự; trường hợp từ chối cấp thì phải thông báo bằng văn bản và nêu rõ lý do.

4. Giấy phép kinh doanh sản phẩm, dịch vụ mật mã dân sự có thời hạn 10 năm.

Điều 33. Sửa đổi, bổ sung, cấp lại, gia hạn, tạm đình chỉ và thu hồi Giấy phép kinh doanh sản phẩm, dịch vụ mật mã dân sự

1. Việc sửa đổi, bổ sung Giấy phép kinh doanh sản phẩm, dịch vụ mật mã dân sự được thực hiện trong trường hợp doanh nghiệp đã được cấp Giấy phép thay đổi

tên, thay đổi người đại diện theo pháp luật hoặc thay đổi, bổ sung sản phẩm, dịch vụ mật mã dân sự.

Doanh nghiệp có trách nhiệm nộp hồ sơ đề nghị sửa đổi, bổ sung Giấy phép tại Ban Cơ yếu Chính phủ. Hồ sơ được lập thành hai bộ, gồm:

a) Đơn đề nghị sửa đổi, bổ sung Giấy phép;

b) Bản sao Giấy chứng nhận đăng ký doanh nghiệp hoặc Giấy chứng nhận đăng ký đầu tư hoặc giấy tờ khác có giá trị tương đương;

c) Giấy phép kinh doanh sản phẩm, dịch vụ mật mã dân sự đã được cấp;

d) Phương án kỹ thuật, phương án bảo mật và an toàn thông tin mạng, phương án kinh doanh đối với sản phẩm, dịch vụ bổ sung theo quy định tại các điểm d, đ và e khoản 2 Điều 32 của Luật này trong trường hợp doanh nghiệp đề nghị bổ sung sản phẩm, dịch vụ mật mã dân sự, ngành, nghề kinh doanh;

Trong thời hạn 10 ngày làm việc kể từ ngày nhận đủ hồ sơ, Ban Cơ yếu Chính phủ thẩm định, sửa đổi, bổ sung và cấp lại Giấy phép cho doanh nghiệp; trường hợp từ chối cấp thì phải thông báo bằng văn bản và nêu rõ lý do.

2. Trường hợp Giấy phép kinh doanh sản phẩm, dịch vụ mật mã dân sự bị mất hoặc bị hư hỏng, doanh nghiệp gửi đơn đề nghị cấp lại Giấy phép, trong đó nêu rõ lý do, tới Ban Cơ yếu Chính phủ. Trong thời hạn 05 ngày làm việc kể từ ngày nhận được đơn đề nghị, Ban Cơ yếu Chính phủ xem xét và cấp lại Giấy phép cho doanh nghiệp.

3. Doanh nghiệp không vi phạm các quy định của pháp luật về kinh doanh sản phẩm, dịch vụ mật mã dân sự được gia hạn Giấy phép kinh doanh sản phẩm, dịch vụ mật mã dân sự một lần với thời gian gia hạn không quá 01 năm.

Hồ sơ đề nghị gia hạn Giấy phép phải được gửi tới Ban Cơ yếu Chính phủ chậm nhất là 60 ngày trước ngày Giấy phép hết hạn. Hồ sơ đề nghị gia hạn Giấy phép được lập thành hai bộ, gồm:

a) Đơn đề nghị gia hạn Giấy phép;

b) Giấy phép kinh doanh sản phẩm, dịch vụ mật mã dân sự đang có hiệu lực;

c) Báo cáo hoạt động của doanh nghiệp trong 02 năm gần nhất.

Trong thời hạn 20 ngày kể từ ngày nhận đủ hồ sơ, Ban Cơ yếu Chính phủ thẩm định, quyết định gia hạn và cấp lại Giấy phép cho doanh nghiệp; trường hợp từ chối cấp thì phải thông báo bằng văn bản và nêu rõ lý do.

4. Doanh nghiệp bị tạm đình chỉ hoạt động kinh doanh sản phẩm, dịch vụ mật mã dân sự có thời hạn không quá 06 tháng trong các trường hợp sau đây:

a) Cung cấp sản phẩm, dịch vụ không đúng với nội dung ghi trên Giấy phép;

b) Không đáp ứng được một trong các điều kiện quy định tại khoản 2 Điều 31 của Luật này;

c) Các trường hợp khác theo quy định của pháp luật.

5. Doanh nghiệp bị thu hồi Giấy phép kinh doanh sản phẩm, dịch vụ mật mã dân sự trong các trường hợp sau đây:

a) Không triển khai cung cấp dịch vụ trong thời hạn 01 năm kể từ ngày được cấp Giấy phép mà không có lý do chính đáng;

b) Giấy phép đã hết hạn;

c) Hết thời hạn tạm đình chỉ mà doanh nghiệp không khắc phục được các lý do quy định tại khoản 4 Điều này.

Điều 34. Xuất khẩu, nhập khẩu sản phẩm mật mã dân sự

1. Khi xuất khẩu, nhập khẩu sản phẩm mật mã dân sự thuộc Danh mục sản phẩm mật mã dân sự xuất khẩu, nhập khẩu theo giấy phép, doanh nghiệp phải có Giấy phép xuất khẩu, nhập khẩu sản phẩm mật mã dân sự do cơ quan nhà nước có thẩm quyền cấp.

2. Doanh nghiệp được cấp Giấy phép xuất khẩu, nhập khẩu sản phẩm mật mã dân sự khi đáp ứng đủ các điều kiện sau đây:

a) Có Giấy phép kinh doanh sản phẩm, dịch vụ mật mã dân sự;

b) Sản phẩm mật mã dân sự nhập khẩu phải được chứng nhận, công bố hợp quy theo quy định tại Điều 39 của Luật này;

c) Đối tượng và mục đích sử dụng sản phẩm mật mã dân sự không gây phương hại đến quốc phòng, an ninh quốc gia và trật tự, an toàn xã hội.

3. Hồ sơ đề nghị cấp Giấy phép xuất khẩu, nhập khẩu sản phẩm mật mã dân sự gồm:

a) Đơn đề nghị cấp Giấy phép xuất khẩu, nhập khẩu sản phẩm mật mã dân sự;

b) Bản sao Giấy phép kinh doanh sản phẩm, dịch vụ mật mã dân sự;

c) Bản sao Giấy chứng nhận hợp quy đối với sản phẩm mật mã dân sự nhập khẩu.

4. Trong thời hạn 10 ngày làm việc kể từ ngày nhận đủ hồ sơ, Ban Cơ yếu Chính phủ thẩm định và cấp Giấy phép xuất khẩu, nhập khẩu sản phẩm mật mã dân sự cho doanh nghiệp; trường hợp từ chối cấp thì phải thông báo bằng văn bản và nêu rõ lý do.

5. Chính phủ ban hành Danh mục sản phẩm mật mã dân sự xuất khẩu, nhập khẩu theo giấy phép và quy định chi tiết Điều này.

Điều 35. Trách nhiệm của doanh nghiệp kinh doanh sản phẩm, dịch vụ mật mã dân sự

1. Quản lý hồ sơ, tài liệu về giải pháp kỹ thuật, công nghệ của sản phẩm.

2. Lập, lưu giữ và bảo mật thông tin của khách hàng, tên, loại hình, số lượng và mục đích sử dụng của sản phẩm, dịch vụ mật mã dân sự.

3. Định kỳ hằng năm báo cáo Ban Cơ yếu Chính phủ về tình hình kinh doanh, xuất khẩu, nhập khẩu sản phẩm, dịch vụ mật mã dân sự và tổng hợp thông tin khách hàng trước ngày 31 tháng 12.

4. Có các biện pháp bảo đảm an ninh, an toàn trong vận chuyển và bảo quản sản phẩm mật mã dân sự.

5. Từ chối cung cấp sản phẩm, dịch vụ mật mã dân sự khi phát hiện tổ chức, cá nhân vi phạm pháp luật về sử dụng sản phẩm, dịch vụ mật mã dân sự, vi phạm cam kết đã thỏa thuận về sử dụng sản phẩm, dịch vụ do doanh nghiệp cung cấp.

6. Tạm ngừng hoặc ngừng cung cấp sản phẩm, dịch vụ mật mã dân sự để bảo đảm quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội theo yêu cầu của cơ quan nhà nước có thẩm quyền.

7. Phối hợp, tạo điều kiện cho cơ quan nhà nước có thẩm quyền thực hiện các biện pháp nghiệp vụ khi có yêu cầu.

Điều 36. Trách nhiệm của tổ chức, cá nhân sử dụng sản phẩm, dịch vụ mật mã dân sự

1. Tuân thủ các quy định đã cam kết với doanh nghiệp cung cấp sản phẩm mật mã dân sự về quản lý sử dụng khóa mã, chuyển nhượng, sửa chữa, bảo dưỡng, bỏ, tiêu hủy sản phẩm mật mã dân sự và các nội dung khác có liên quan.

2. Cung cấp các thông tin cần thiết liên quan tới khóa mã cho cơ quan nhà nước có thẩm quyền khi có yêu cầu.

3. Phối hợp, tạo điều kiện cho cơ quan nhà nước có thẩm quyền thực hiện các biện pháp ngăn ngừa tội phạm đánh cắp thông tin, khóa mã và sử dụng sản phẩm mật mã dân sự vào những mục đích không hợp pháp.

4. Tổ chức, cá nhân sử dụng sản phẩm mật mã dân sự không do doanh nghiệp được cấp phép kinh doanh sản phẩm mật mã dân sự cung cấp phải khai báo với Ban Cơ yếu Chính phủ, trừ cơ quan đại diện ngoại giao, cơ quan lãnh sự của nước ngoài và cơ quan đại diện của tổ chức quốc tế liên Chính phủ tại Việt Nam.

Chương IV
TIÊU CHUẨN, QUY CHUẨN KỸ THUẬT AN TOÀN THÔNG TIN MẠNG

Điều 37. Tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin mạng

1. Tiêu chuẩn an toàn thông tin mạng gồm tiêu chuẩn quốc tế, tiêu chuẩn khu vực, tiêu chuẩn nước ngoài, tiêu chuẩn quốc gia và tiêu chuẩn cơ sở đối với hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an toàn thông tin mạng được công bố, thừa nhận áp dụng tại Việt Nam.

2. Quy chuẩn kỹ thuật an toàn thông tin mạng gồm quy chuẩn kỹ thuật quốc gia và quy chuẩn kỹ thuật địa phương đối với hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an toàn thông tin mạng được xây dựng, ban hành và áp dụng tại Việt Nam.

Điều 38. Quản lý tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin mạng

1. Chứng nhận hợp quy về an toàn thông tin mạng là việc tổ chức chứng nhận sự phù hợp chứng nhận hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an toàn thông tin mạng phù hợp với quy chuẩn kỹ thuật an toàn thông tin mạng.

2. Công bố hợp quy về an toàn thông tin mạng là việc tổ chức, doanh nghiệp công bố về sự phù hợp của hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an toàn thông tin mạng với quy chuẩn kỹ thuật an toàn thông tin mạng.

3. Chứng nhận hợp chuẩn về an toàn thông tin mạng là việc tổ chức chứng nhận sự phù hợp chứng nhận hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an toàn thông tin mạng phù hợp với tiêu chuẩn an toàn thông tin mạng.

4. Công bố hợp chuẩn về an toàn thông tin mạng là việc tổ chức, doanh nghiệp công bố về sự phù hợp của hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an toàn thông tin mạng với tiêu chuẩn an toàn thông tin mạng.

5. Bộ Khoa học và Công nghệ chủ trì, phối hợp với cơ quan có liên quan tổ chức thẩm định và công bố tiêu chuẩn quốc gia về an toàn thông tin mạng theo quy định của pháp luật về tiêu chuẩn, quy chuẩn kỹ thuật.

6. Bộ Thông tin và Truyền thông có trách nhiệm sau đây:

a) Xây dựng dự thảo tiêu chuẩn quốc gia an toàn thông tin mạng, trừ tiêu chuẩn quốc gia quy định tại khoản 7 Điều này;

b) Ban hành quy chuẩn kỹ thuật quốc gia an toàn thông tin mạng, trừ quy chuẩn quốc gia quy định tại khoản 7 Điều này; quy định về đánh giá hợp quy về an toàn thông tin mạng;

c) Quản lý chất lượng sản phẩm, dịch vụ an toàn thông tin mạng, trừ sản phẩm, dịch vụ mật mã dân sự;

d) Đăng ký, chỉ định và quản lý hoạt động của tổ chức chứng nhận sự phù hợp về an toàn thông tin mạng, trừ tổ chức chứng nhận sự phù hợp đối với sản phẩm, dịch vụ mật mã dân sự.

7. Ban Cơ yếu Chính phủ có trách nhiệm giúp Bộ trưởng Bộ Quốc phòng xây dựng dự thảo tiêu chuẩn quốc gia đối với sản phẩm, dịch vụ mật mã dân sự trình cơ quan nhà nước có thẩm quyền công bố và hướng dẫn thực hiện; xây dựng, trình Bộ trưởng Bộ Quốc phòng ban hành quy chuẩn kỹ thuật quốc gia đối với sản phẩm, dịch vụ mật mã dân sự, chỉ định và quản lý hoạt động của tổ chức chứng nhận sự phù hợp đối với sản phẩm, dịch vụ mật mã dân sự; quản lý chất lượng sản phẩm, dịch vụ mật mã dân sự.

8. Ủy ban nhân dân cấp tỉnh xây dựng, ban hành và hướng dẫn thực hiện quy chuẩn kỹ thuật địa phương về an toàn thông tin mạng; quản lý chất lượng sản phẩm, dịch vụ an toàn thông tin mạng trên địa bàn.

Điều 39. Đánh giá hợp chuẩn, hợp quy về an toàn thông tin mạng

1. Việc đánh giá hợp chuẩn, hợp quy về an toàn thông tin mạng được thực hiện trong các trường hợp sau đây:

a) Trước khi tổ chức, cá nhân đưa sản phẩm an toàn thông tin mạng vào lưu thông trên thị trường phải thực hiện chứng nhận hợp quy hoặc công bố hợp quy và sử dụng dấu hợp quy;

b) Phục vụ hoạt động quản lý nhà nước về an toàn thông tin mạng.

2. Việc đánh giá hợp chuẩn, hợp quy về an toàn thông tin mạng phục vụ hệ thống thông tin quan trọng quốc gia và phục vụ hoạt động quản lý nhà nước về an toàn thông tin mạng được thực hiện tại tổ chức chứng nhận sự phù hợp do Bộ trưởng Bộ Thông tin và Truyền thông chỉ định.

3. Việc đánh giá hợp chuẩn, hợp quy đối với sản phẩm, dịch vụ mật mã dân sự được thực hiện tại tổ chức chứng nhận sự phù hợp do Bộ trưởng Bộ Quốc phòng chỉ định.

4. Việc thừa nhận kết quả đánh giá hợp chuẩn, hợp quy về an toàn thông tin mạng giữa Việt Nam với quốc gia, vùng lãnh thổ khác, giữa tổ chức chứng nhận sự phù hợp của Việt Nam với tổ chức chứng nhận sự phù hợp của quốc gia, vùng lãnh thổ khác được thực hiện theo quy định của pháp luật về tiêu chuẩn, quy chuẩn kỹ thuật.

Chương V
KINH DOANH TRONG LĨNH VỰC AN TOÀN THÔNG TIN MẠNG

Mục 1
CẤP GIẤY PHÉP KINH DOANH SẢN PHẨM, DỊCH VỤ AN TOÀN THÔNG TIN MẠNG

Điều 40. Kinh doanh trong lĩnh vực an toàn thông tin mạng

1. Kinh doanh trong lĩnh vực an toàn thông tin mạng là ngành, nghề kinh doanh có điều kiện. Kinh doanh trong lĩnh vực an toàn thông tin mạng gồm kinh doanh sản phẩm an toàn thông tin mạng và kinh doanh dịch vụ an toàn thông tin mạng.

2. Doanh nghiệp kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng quy định tại Điều 41 của Luật này phải có Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng do cơ quan nhà nước có thẩm quyền cấp. Thời hạn của Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng là 10 năm.

3. Việc kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng phải tuân thủ quy định của Luật này và quy định khác của pháp luật có liên quan.

Điều kiện kinh doanh, trình tự thủ tục cấp Giấy phép kinh doanh sản phẩm, dịch vụ mật mã dân sự, việc xuất khẩu, nhập khẩu sản phẩm mật mã dân sự, trách nhiệm của doanh nghiệp kinh doanh sản phẩm, dịch vụ mật mã dân sự và việc sử dụng sản phẩm, dịch vụ mật mã dân sự thực hiện theo quy định tại Chương III của Luật này.

Điều kiện kinh doanh, trình tự, thủ tục cấp Giấy phép kinh doanh dịch vụ chứng thực chữ ký điện tử thực hiện theo quy định của pháp luật về giao dịch điện tử.

Điều 41. Sản phẩm, dịch vụ trong lĩnh vực an toàn thông tin mạng

1. Dịch vụ an toàn thông tin mạng gồm:

a) Dịch vụ kiểm tra, đánh giá an toàn thông tin mạng;

b) Dịch vụ bảo mật thông tin không sử dụng mật mã dân sự;

c) Dịch vụ mật mã dân sự;

d) Dịch vụ chứng thực chữ ký điện tử;

đ) Dịch vụ tư vấn an toàn thông tin mạng;

e) Dịch vụ giám sát an toàn thông tin mạng;

g) Dịch vụ ứng cứu sự cố an toàn thông tin mạng;

h) Dịch vụ khôi phục dữ liệu;

i) Dịch vụ phòng ngừa, chống tấn công mạng;

k) Dịch vụ an toàn thông tin mạng khác.

2. Sản phẩm an toàn thông tin mạng gồm:

a) Sản phẩm mật mã dân sự;

b) Sản phẩm kiểm tra, đánh giá an toàn thông tin mạng;

c) Sản phẩm giám sát an toàn thông tin mạng;

d) Sản phẩm chống tấn công, xâm nhập;

đ) Sản phẩm an toàn thông tin mạng khác.

3. Chính phủ quy định chi tiết danh mục sản phẩm, dịch vụ an toàn thông tin mạng quy định tại điểm k khoản 1 và điểm đ khoản 2 Điều này.

Điều 42. Điều kiện cấp Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng

1. Doanh nghiệp được cấp Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng, trừ sản phẩm, dịch vụ quy định tại các điểm a, b, c, d khoản 1 và điểm a khoản 2 Điều 41 của Luật này, khi đáp ứng đủ các điều kiện sau đây:

a) Phù hợp với chiến lược,[2] kế hoạch phát triển an toàn thông tin mạng quốc gia;

b) Có hệ thống trang thiết bị, cơ sở vật chất phù hợp với quy mô cung cấp sản phẩm, dịch vụ an toàn thông tin mạng;

c) Có đội ngũ quản lý, điều hành, kỹ thuật đáp ứng được yêu cầu chuyên môn về an toàn thông tin;

d) Có phương án kinh doanh phù hợp.

2. Doanh nghiệp được cấp Giấy phép kinh doanh dịch vụ kiểm tra, đánh giá an toàn thông tin mạng khi đáp ứng đủ các điều kiện sau đây:

a) Các điều kiện quy định tại khoản 1 Điều này;

b) Là doanh nghiệp được thành lập và hoạt động hợp pháp trên lãnh thổ Việt Nam, trừ doanh nghiệp có vốn đầu tư nước ngoài;

---

[2] Từ "quy hoạch," được bãi bỏ theo quy định tại khoản 3 Điều 18 của Luật số 35/2018/QH14 sửa đổi, bổ sung một số điều của 37 luật có liên quan đến quy hoạch, có hiệu lực kể từ ngày 01 tháng 01 năm 2019.

c) Người đại diện theo pháp luật, đội ngũ quản lý, điều hành, kỹ thuật là công dân Việt Nam thường trú tại Việt Nam;

d) Có phương án kỹ thuật phù hợp với tiêu chuẩn, quy chuẩn kỹ thuật;

đ) Có phương án bảo mật thông tin khách hàng trong quá trình cung cấp dịch vụ;

e) Đội ngũ quản lý, điều hành, kỹ thuật có văn bằng hoặc chứng chỉ chuyên môn về kiểm tra, đánh giá an toàn thông tin.

3. Doanh nghiệp được cấp Giấy phép kinh doanh dịch vụ bảo mật thông tin không sử dụng mật mã dân sự khi đáp ứng đủ các điều kiện sau đây:

a) Các điều kiện quy định tại các điểm a, b, c, d và đ khoản 2 Điều này;

b) Đội ngũ quản lý điều hành, kỹ thuật có văn bằng hoặc chứng chỉ chuyên môn về bảo mật thông tin.

4. Chính phủ quy định chi tiết Điều này.

Điều 43. Hồ sơ đề nghị cấp Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng

1. Doanh nghiệp đề nghị cấp Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng nộp hồ sơ đề nghị cấp Giấy phép tại Bộ Thông tin và Truyền thông.

2. Hồ sơ đề nghị cấp Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng được lập thành năm bộ, gồm:

a) Đơn đề nghị cấp Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng, trong đó nêu rõ loại hình sản phẩm, dịch vụ an toàn thông tin mạng sẽ kinh doanh;

b) Bản sao Giấy chứng nhận đăng ký doanh nghiệp, Giấy chứng nhận đăng ký đầu tư hoặc giấy tờ khác có giá trị tương đương;

c) Bản thuyết minh hệ thống thiết bị kỹ thuật bảo đảm phù hợp với quy định của pháp luật;

d) Phương án kinh doanh gồm phạm vi, đối tượng cung cấp sản phẩm, dịch vụ, tiêu chuẩn, chất lượng sản phẩm, dịch vụ;

đ) Bản sao văn bằng hoặc chứng chỉ chuyên môn về an toàn thông tin của đội ngũ quản lý, điều hành, kỹ thuật.

3. Ngoài giấy tờ, tài liệu quy định tại khoản 2 Điều này, hồ sơ đề nghị cấp Giấy phép kinh doanh dịch vụ kiểm tra, đánh giá an toàn thông tin hoặc dịch vụ bảo mật thông tin không sử dụng mật mã dân sự còn phải có:

a) Phiếu lý lịch tư pháp của người đại diện theo pháp luật và đội ngũ quản lý, điều hành, kỹ thuật;

b) Phương án kỹ thuật;

c) Phương án bảo mật thông tin khách hàng trong quá trình cung cấp dịch vụ.

Điều 44. Thẩm định hồ sơ và cấp Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng

1. Trong thời hạn 40 ngày kể từ ngày nhận đủ hồ sơ, Bộ Thông tin và Truyền thông chủ trì, phối hợp với bộ, ngành có liên quan thẩm định và cấp Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng, trừ kinh doanh sản phẩm, dịch vụ quy định tại điểm c, điểm d khoản 1 và điểm a khoản 2 Điều 41 của Luật này; trường hợp từ chối cấp thì phải thông báo bằng văn bản và nêu rõ lý do.

2. Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng có nội dung chính sau đây:

a) Tên doanh nghiệp, tên giao dịch của doanh nghiệp bằng tiếng Việt và tiếng nước ngoài (nếu có); địa chỉ trụ sở chính tại Việt Nam;

b) Tên của người đại diện theo pháp luật;

c) Số giấy phép, ngày cấp giấy phép, ngày hết hạn giấy phép;

d) Sản phẩm, dịch vụ an toàn thông tin mạng được phép kinh doanh.

3. Doanh nghiệp được cấp Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng phải nộp phí theo quy định của pháp luật về phí và lệ phí.

Điều 45. Sửa đổi, bổ sung, gia hạn, tạm đình chỉ, thu hồi và cấp lại Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng

1. Việc sửa đổi, bổ sung Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng được thực hiện trong trường hợp doanh nghiệp đã được cấp Giấy phép thay đổi tên, thay đổi người đại diện theo pháp luật hoặc thay đổi, bổ sung sản phẩm, dịch vụ an toàn thông tin mạng mà mình cung cấp.

Doanh nghiệp có trách nhiệm nộp hồ sơ đề nghị sửa đổi, bổ sung nội dung Giấy phép tại Bộ Thông tin và Truyền thông. Hồ sơ được lập thành hai bộ, gồm đơn đề nghị sửa đổi, bổ sung nội dung Giấy phép, báo cáo mô tả chi tiết nội dung đề nghị sửa đổi, bổ sung và các tài liệu khác có liên quan.

Trong thời hạn 10 ngày làm việc kể từ ngày nhận đủ hồ sơ, Bộ Thông tin và Truyền thông thẩm định, sửa đổi, bổ sung và cấp lại Giấy phép cho doanh nghiệp; trường hợp từ chối cấp thì phải thông báo bằng văn bản và nêu rõ lý do.

2. Trường hợp Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin bị mất hoặc bị hư hỏng, doanh nghiệp gửi đơn đề nghị cấp lại Giấy phép, trong đó nêu rõ lý do, tới Bộ Thông tin và Truyền thông. Trong thời hạn 05 ngày làm việc kể từ ngày nhận được đơn đề nghị, Bộ Thông tin và Truyền thông xem xét và cấp lại Giấy phép cho doanh nghiệp.

3. Doanh nghiệp không vi phạm quy định của pháp luật về kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng được gia hạn Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng một lần với thời gian gia hạn không quá 01 năm. Hồ sơ đề nghị gia hạn Giấy phép phải được gửi tới Bộ Thông tin và Truyền thông chậm nhất là 60 ngày trước ngày Giấy phép hết hạn. Hồ sơ đề nghị gia hạn Giấy phép được lập thành hai bộ, gồm:

a) Đơn đề nghị gia hạn Giấy phép;

b) Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng đang có hiệu lực;

c) Báo cáo hoạt động của doanh nghiệp trong 02 năm gần nhất.

Trong thời hạn 20 ngày kể từ ngày nhận đủ hồ sơ, Bộ Thông tin và Truyền thông thẩm định, quyết định gia hạn và cấp lại Giấy phép cho doanh nghiệp; trường hợp từ chối cấp thì phải thông báo bằng văn bản và nêu rõ lý do.

4. Doanh nghiệp bị tạm đình chỉ hoạt động kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng có thời hạn không quá 06 tháng trong các trường hợp sau đây:

a) Cung cấp dịch vụ không đúng với nội dung ghi trên Giấy phép;

b) Không đáp ứng được một trong các điều kiện quy định tại Điều 42 của Luật này;

c) Các trường hợp khác theo quy định của pháp luật.

5. Doanh nghiệp bị thu hồi Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng trong các trường hợp sau đây:

a) Không triển khai cung cấp dịch vụ trong thời hạn 01 năm kể từ ngày được cấp Giấy phép mà không có lý do chính đáng;

b) Giấy phép đã hết hạn;

c) Hết thời hạn tạm đình chỉ mà doanh nghiệp không khắc phục được các lý do quy định tại khoản 4 Điều này.

Điều 46. Trách nhiệm của doanh nghiệp kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng

1. Quản lý hồ sơ, tài liệu về giải pháp kỹ thuật, công nghệ của sản phẩm.

2. Lập, lưu giữ và bảo mật thông tin của khách hàng.

3. Định kỳ hằng năm báo cáo Bộ Thông tin và Truyền thông về tình hình kinh doanh, xuất khẩu, nhập khẩu sản phẩm, dịch vụ an toàn thông tin mạng trước ngày 31 tháng 12.

4. Từ chối cung cấp sản phẩm, dịch vụ an toàn thông tin mạng khi phát hiện tổ chức, cá nhân vi phạm pháp luật về sử dụng sản phẩm, dịch vụ an toàn thông tin mạng, vi phạm cam kết đã thỏa thuận về sử dụng sản phẩm, dịch vụ do doanh nghiệp cung cấp.

5. Tạm ngừng hoặc ngừng cung cấp sản phẩm, dịch vụ an toàn thông tin mạng để bảo đảm quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội theo yêu cầu của cơ quan nhà nước có thẩm quyền.

6. Phối hợp, tạo điều kiện cho cơ quan nhà nước có thẩm quyền thực hiện các biện pháp nghiệp vụ khi có yêu cầu.

Mục 2
QUẢN LÝ NHẬP KHẨU SẢN PHẨM AN TOÀN THÔNG TIN MẠNG

Điều 47. Nguyên tắc quản lý nhập khẩu sản phẩm an toàn thông tin mạng

1. Việc quản lý nhập khẩu đối với sản phẩm an toàn thông tin mạng được thực hiện theo quy định của Luật này và quy định khác của pháp luật có liên quan.

2. Việc nhập khẩu sản phẩm an toàn thông tin mạng của cơ quan, tổ chức, cá nhân được hưởng quyền ưu đãi, miễn trừ ngoại giao thực hiện theo quy định của pháp luật về hải quan, pháp luật về ưu đãi, miễn trừ dành cho cơ quan đại diện ngoại giao, cơ quan lãnh sự của nước ngoài và cơ quan đại diện của tổ chức quốc tế liên Chính phủ tại Việt Nam.

3. Trong trường hợp Việt Nam chưa có quy chuẩn kỹ thuật an toàn thông tin mạng tương ứng đối với sản phẩm an toàn thông tin mạng nhập khẩu thì áp dụng theo thỏa thuận quốc tế, điều ước quốc tế mà Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên.

Điều 48. Sản phẩm nhập khẩu theo giấy phép trong lĩnh vực an toàn thông tin mạng

1. Khi nhập khẩu sản phẩm an toàn thông tin mạng thuộc Danh mục sản phẩm an toàn thông tin mạng nhập khẩu theo giấy phép do Chính phủ quy định, doanh nghiệp phải có Giấy phép nhập khẩu sản phẩm an toàn thông tin mạng do cơ quan nhà nước có thẩm quyền cấp.

2. Tổ chức, doanh nghiệp nhập khẩu sản phẩm an toàn thông tin mạng phải thực hiện chứng nhận, công bố hợp quy trước khi nhập khẩu theo quy định tại Điều 39 của Luật này.

3. Tổ chức, doanh nghiệp được cấp Giấy phép nhập khẩu sản phẩm an toàn thông tin mạng khi đáp ứng đủ các điều kiện sau đây:

a) Có Giấy phép kinh doanh sản phẩm an toàn thông tin mạng;

b) Sản phẩm an toàn thông tin mạng phải thực hiện chứng nhận, công bố hợp quy theo quy định tại Điều 39 của Luật này;

c) Đối tượng và mục đích sử dụng sản phẩm an toàn thông tin mạng không gây phương hại đến quốc phòng, an ninh quốc gia và trật tự, an toàn xã hội.

4. Bộ Thông tin và Truyền thông quy định chi tiết về trình tự, thủ tục, hồ sơ cấp Giấy phép nhập khẩu sản phẩm an toàn thông tin mạng theo giấy phép.

Chương VI
PHÁT TRIỂN NGUỒN NHÂN LỰC AN TOÀN THÔNG TIN MẠNG

Điều 49. Đào tạo, bồi dưỡng nghiệp vụ về an toàn thông tin mạng

1. Chủ quản hệ thống thông tin có trách nhiệm đào tạo và bồi dưỡng kiến thức, nghiệp vụ cho cán bộ quản lý, kỹ thuật về an toàn thông tin mạng.

2. Cán bộ chuyên trách về an toàn thông tin mạng được bố trí, tạo điều kiện làm việc phù hợp với chuyên môn, được ưu tiên bồi dưỡng nghiệp vụ về an toàn thông tin mạng.

3. Nhà nước khuyến khích tổ chức, cá nhân đầu tư, liên doanh, liên kết với tổ chức khác để đầu tư xây dựng cơ sở giáo dục đại học, cơ sở giáo dục nghề nghiệp nhằm đào tạo nhân lực trong lĩnh vực an toàn thông tin mạng.

4. Bộ Nội vụ chủ trì, phối hợp với Bộ Thông tin và Truyền thông, bộ, ngành có liên quan xây dựng kế hoạch và tổ chức thực hiện đào tạo, bồi dưỡng kiến thức, nghiệp vụ về an toàn thông tin mạng cho cán bộ, công chức, viên chức.

Điều 50. Văn bằng, chứng chỉ đào tạo về an toàn thông tin mạng

1. Cơ sở giáo dục đại học, cơ sở giáo dục nghề nghiệp trong phạm vi nhiệm vụ, quyền hạn của mình cấp văn bằng, chứng chỉ đào tạo về an toàn thông tin mạng.

2. Bộ Giáo dục và Đào tạo chủ trì, phối hợp với Bộ Thông tin và Truyền thông, bộ, ngành có liên quan công nhận văn bằng giáo dục đại học về an toàn thông tin mạng do tổ chức nước ngoài cấp.

3. Bộ Lao động - Thương binh và Xã hội chủ trì, phối hợp với Bộ Thông tin và Truyền thông, bộ, ngành có liên quan công nhận văn bằng, chứng chỉ giáo dục nghề nghiệp về an toàn thông tin mạng do tổ chức nước ngoài cấp.

Chương VII
QUẢN LÝ NHÀ NƯỚC VỀ AN TOÀN THÔNG TIN MẠNG

Điều 51. Nội dung quản lý nhà nước về an toàn thông tin mạng

1.[3] Xây dựng chiến lược, kế hoạch và chính sách trong lĩnh vực an toàn thông tin mạng; xây dựng và chỉ đạo thực hiện chương trình quốc gia về an toàn thông tin mạng; tổ chức lập phương án phát triển hạ tầng bảo đảm an toàn thông tin mạng trong quy hoạch hạ tầng thông tin và truyền thông, quy hoạch khác có liên quan theo quy định của pháp luật về quy hoạch.

2. Ban hành và tổ chức thực hiện văn bản quy phạm pháp luật về an toàn thông tin mạng; xây dựng, công bố tiêu chuẩn quốc gia, ban hành quy chuẩn kỹ thuật về an toàn thông tin mạng.

3. Quản lý nhà nước về mật mã dân sự.

4. Quản lý công tác đánh giá, công bố hợp chuẩn, hợp quy về an toàn thông tin mạng.

5. Quản lý công tác giám sát an toàn hệ thống thông tin.

6. Thẩm định về an toàn thông tin mạng trong hồ sơ thiết kế hệ thống thông tin.

7. Tuyên truyền, phổ biến pháp luật về an toàn thông tin mạng.

8. Quản lý hoạt động kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng.

9. Tổ chức nghiên cứu, ứng dụng khoa học và công nghệ về an toàn thông tin mạng; phát triển nguồn nhân lực an toàn thông tin mạng; đào tạo cán bộ chuyên trách về an toàn thông tin mạng.

10. Kiểm tra, thanh tra, giải quyết khiếu nại, tố cáo, xử lý vi phạm pháp luật về an toàn thông tin mạng.

11. Hợp tác quốc tế về an toàn thông tin mạng.

Điều 52. Trách nhiệm quản lý nhà nước về an toàn thông tin mạng

1. Chính phủ thống nhất quản lý nhà nước về an toàn thông tin mạng.

2. Bộ Thông tin và Truyền thông chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về an toàn thông tin mạng, có nhiệm vụ, quyền hạn sau đây:

---

[3] Khoản này được sửa đổi, bổ sung theo quy định tại khoản 1 Điều 18 của Luật số 35/2018/QH14 sửa đổi, bổ sung một số điều của 37 luật có liên quan đến quy hoạch, có hiệu lực kể từ ngày 01 tháng 01 năm 2019.

a)[4] Ban hành hoặc xây dựng, trình cấp có thẩm quyền ban hành văn bản quy phạm pháp luật, chiến lược, kế hoạch, tiêu chuẩn quốc gia, quy chuẩn kỹ thuật quốc gia về an toàn thông tin mạng; tổ chức lập phương án phát triển hạ tầng bảo đảm an toàn thông tin mạng trong quy hoạch hạ tầng thông tin và truyền thông, quy hoạch khác có liên quan theo quy định của pháp luật về quy hoạch;

b) Thẩm định về an toàn thông tin mạng trong hồ sơ thiết kế hệ thống thông tin;

c) Quản lý công tác giám sát an toàn hệ thống thông tin trên toàn quốc, trừ hệ thống thông tin quy định tại điểm c khoản 3 và điểm b khoản 5 Điều này;

d) Quản lý công tác đánh giá về an toàn thông tin mạng;

đ) Cấp Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng, Giấy phép nhập khẩu sản phẩm an toàn thông tin, trừ sản phẩm, dịch vụ mật mã dân sự;

e) Nghiên cứu, ứng dụng khoa học và công nghệ về an toàn thông tin mạng; đào tạo, bồi dưỡng, phát triển nguồn nhân lực;

g) Quản lý và thực hiện hợp tác quốc tế về an toàn thông tin mạng;

h) Kiểm tra, thanh tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm pháp luật về an toàn thông tin mạng;

i) Chủ trì, phối hợp với bộ, ngành, Ủy ban nhân dân cấp tỉnh và doanh nghiệp có liên quan trong việc bảo đảm an toàn thông tin mạng;

k) Tổ chức tuyên truyền, phổ biến pháp luật về an toàn thông tin mạng;

l) Định kỳ hằng năm báo cáo Chính phủ về hoạt động an toàn thông tin mạng.

3. Bộ Quốc phòng có nhiệm vụ, quyền hạn sau đây:

a) Ban hành hoặc xây dựng, trình cấp có thẩm quyền ban hành văn bản quy phạm pháp luật, chiến lược,[5] kế hoạch, tiêu chuẩn quốc gia, quy chuẩn kỹ thuật quốc gia về an toàn thông tin mạng thuộc lĩnh vực do Bộ Quốc phòng quản lý;

b) Kiểm tra, thanh tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm pháp luật trong hoạt động bảo đảm an toàn thông tin mạng thuộc lĩnh vực do Bộ Quốc phòng quản lý;

c) Thực hiện quản lý công tác giám sát an toàn hệ thống thông tin thuộc Bộ Quốc phòng.

---

[4] Điểm này được sửa đổi, bổ sung theo quy định tại khoản 2 Điều 18 của Luật số 35/2018/QH14 sửa đổi, bổ sung một số điều của 37 luật có liên quan đến quy hoạch, có hiệu lực kể từ ngày 01 tháng 01 năm 2019.

[5] Từ "quy hoạch," được bãi bỏ theo quy định tại khoản 3 Điều 18 của Luật số 35/2018/QH14 sửa đổi, bổ sung một số điều của 37 luật có liên quan đến quy hoạch, có hiệu lực kể từ ngày 01 tháng 01 năm 2019.

4. Ban Cơ yếu Chính phủ giúp Bộ trưởng Bộ Quốc phòng thực hiện quản lý nhà nước về mật mã dân sự, có nhiệm vụ sau đây:

a) Xây dựng, trình cấp có thẩm quyền ban hành văn bản quy phạm pháp luật về quản lý mật mã dân sự;

b) Chủ trì, phối hợp với bộ, ngành có liên quan xây dựng, trình cơ quan nhà nước có thẩm quyền ban hành tiêu chuẩn quốc gia, quy chuẩn kỹ thuật quốc gia đối với sản phẩm, dịch vụ mật mã dân sự;

c) Quản lý hoạt động kinh doanh, sử dụng mật mã dân sự; quản lý chất lượng sản phẩm, dịch vụ mật mã dân sự; quản lý công tác đánh giá, công bố hợp chuẩn, hợp quy đối với sản phẩm, dịch vụ mật mã dân sự;

d) Xây dựng, trình cấp có thẩm quyền ban hành Danh mục sản phẩm, dịch vụ mật mã dân sự và Danh mục sản phẩm mật mã dân sự xuất khẩu, nhập khẩu theo giấy phép;

đ) Cấp Giấy phép kinh doanh sản phẩm, dịch vụ mật mã dân sự, Giấy phép xuất khẩu, nhập khẩu sản phẩm mật mã dân sự;

e) Kiểm tra, thanh tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm pháp luật trong hoạt động kinh doanh, sử dụng mật mã dân sự;

g) Hợp tác quốc tế về mật mã dân sự.

5. Bộ Công an có nhiệm vụ, quyền hạn sau đây:

a) Chủ trì, phối hợp với bộ, ngành có liên quan xây dựng và trình cấp có thẩm quyền ban hành hoặc ban hành theo thẩm quyền và hướng dẫn thực hiện văn bản quy phạm pháp luật về bảo vệ bí mật nhà nước, phòng, chống tội phạm mạng, lợi dụng mạng để xâm phạm an ninh quốc gia, trật tự, an toàn xã hội;

b) Thực hiện quản lý công tác giám sát an toàn hệ thống thông tin thuộc Bộ Công an;

c) Tổ chức, chỉ đạo, triển khai công tác phòng, chống tội phạm, tổ chức điều tra tội phạm mạng và hành vi vi phạm pháp luật khác trong lĩnh vực an toàn thông tin mạng;

d) Phối hợp với Bộ Thông tin và Truyền thông, bộ, ngành có liên quan kiểm tra, thanh tra về an toàn thông tin mạng, xử lý vi phạm pháp luật về an toàn thông tin mạng theo thẩm quyền.

6. Bộ Nội vụ có trách nhiệm tổ chức đào tạo, bồi dưỡng kiến thức, nghiệp vụ an toàn thông tin mạng cho cán bộ, công chức, viên chức.

7. Bộ Giáo dục và Đào tạo có trách nhiệm tổ chức đào tạo, phổ biến kiến thức về an toàn thông tin mạng trong cơ sở giáo dục đại học.

8. Bộ Lao động - Thương binh và Xã hội có trách nhiệm tổ chức đào tạo, bồi dưỡng, phổ biến kiến thức về an toàn thông tin mạng trong cơ sở giáo dục nghề nghiệp.

9. Bộ Tài chính có trách nhiệm hướng dẫn, bố trí kinh phí thực hiện nhiệm vụ bảo đảm an toàn thông tin mạng theo quy định của pháp luật.

10. Bộ, cơ quan ngang bộ trong phạm vi nhiệm vụ, quyền hạn của mình có trách nhiệm quản lý an toàn thông tin mạng của ngành mình và phối hợp với Bộ Thông tin và Truyền thông thực hiện quản lý nhà nước về an toàn thông tin mạng.

11. Ủy ban nhân dân cấp tỉnh trong phạm vi nhiệm vụ, quyền hạn của mình thực hiện quản lý nhà nước về an toàn thông tin mạng ở địa phương.

Chương VIII
ĐIỀU KHOẢN THI HÀNH[6]

Điều 53. Hiệu lực thi hành

Luật này có hiệu lực thi hành từ ngày 01 tháng 7 năm 2016.

Điều 54. Quy định chi tiết

Chính phủ, cơ quan nhà nước có thẩm quyền quy định chi tiết các điều, khoản được giao trong Luật./.

VĂN PHÒNG QUỐC HỘI

Số: 29/VBHN-VPQH

XÁC THỰC VĂN BẢN HỢP NHẤT

Hà Nội, ngày 10 tháng 12 năm 2018
CHỦ NHIỆM

Nguyễn Hạnh Phúc

---

[6] Điều 31 của Luật số 35/2018/QH14 sửa đổi, bổ sung một số điều của 37 luật có liên quan đến quy hoạch, có hiệu lực kể từ ngày 01 tháng 01 năm 2019 quy định như sau:

"***Điều 31. Hiệu lực thi hành***

Luật này có hiệu lực thi hành từ ngày 01 tháng 01 năm 2019."