2. Bộ trưởng Bộ Công an trực tiếp quyết định đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin, tạm ngừng, thu hồi tên miền có hoạt động vi phạm pháp luật về an ninh mạng.

3. Cục trưởng Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an có trách nhiệm thực hiện quyết định đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin, tạm ngừng, thu hồi tên miền.

4. Trình tự, thủ tục thực hiện biện pháp:

a) Báo cáo về việc áp dụng biện pháp đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin, tạm ngừng, thu hồi tên miền;

b) Quyết định đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin, tạm ngừng, thu hồi tên miền;

c) Gửi văn bản yêu cầu các cơ quan, tổ chức, cá nhân có liên quan thực hiện đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin hoặc gửi Trung tâm Internet Việt Nam đề nghị tạm ngừng, thu hồi tên miền theo trình tự, thủ tục được pháp luật quy định; văn bản yêu cầu nêu rõ lý do, thời gian, nội dung và kiến nghị;

d) Trong trường hợp cấp bách, cần ngăn chặn kịp thời hoạt động của hệ thống thông tin tránh gây nguy hại cho an ninh quốc gia hoặc cần ngăn chặn hậu quả tác hại có thể xảy ra, Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an yêu cầu trực tiếp hoặc bằng văn bản qua fax, email để yêu cầu cơ quan, tổ chức, cá nhân đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin;

Trong thời gian chậm nhất là 24 giờ kể từ khi có yêu cầu, Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an phải gửi văn bản yêu cầu đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin. Trường hợp quá thời hạn trên mà không có quyết định bằng văn bản thì hệ thống thông tin được tiếp tục hoạt động. Tùy theo tính chất, mức độ, hậu quả xảy ra do việc chậm trễ gửi văn bản yêu cầu, cán bộ thực hiện và những người có liên quan phải chịu trách nhiệm theo quy định của pháp luật;

đ) Việc đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin phải được lập thành biên bản. Biên bản phải ghi rõ thời gian, địa điểm, căn cứ và được lập thành 02 bản. Cơ quan chức năng có thẩm quyền giữ một bản, cơ quan, tổ chức, cá nhân sở hữu, quản lý hệ thống thông tin giữ một bản;

e) Việc tạm ngừng, thu hồi tên miền quốc gia trong các trường hợp quy định tại khoản 1 Điều này, cơ quan chức năng có thẩm quyền gửi văn bản đề nghị Trung tâm Internet Việt Nam tạm ngừng, thu hồi tên miền theo trình tự, thủ tục được pháp luật quy định.

5. Việc đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin mà không có căn cứ được quy định tại khoản 2 Điều này thì Thủ trưởng, Phó Thủ trưởng cơ quan chức năng có thẩm quyền và cán bộ có liên quan phải chịu trách nhiệm trước pháp luật, nếu gây thiệt hại cho cơ quan, tổ chức, cá nhân có liên quan thì phải bồi thường theo quy định của pháp luật.

Điều 22. Trách nhiệm của cơ quan, tổ chức, cá nhân trong triển khai các biện pháp bảo vệ an ninh mạng

1. Lực lượng chuyên trách bảo vệ an ninh mạng có trách nhiệm hướng dẫn cụ thể các cơ quan, tổ chức, cá nhân có liên quan thực hiện các quy định về trình tự, thủ tục áp dụng một số biện pháp bảo vệ an ninh mạng.

2. Các cơ quan, tổ chức, cá nhân trong phạm vi trách nhiệm, quyền hạn của mình, kịp thời phối hợp, hỗ trợ lực lượng chuyên trách bảo vệ an ninh mạng thực hiện các quy định về trình tự, thủ tục áp dụng một số biện pháp bảo vệ an ninh mạng.

3. Trường hợp doanh nghiệp cung cấp dịch vụ qua biên giới bị cơ quan có thẩm quyền công bố vi phạm pháp luật Việt Nam, tổ chức, doanh nghiệp Việt Nam có trách nhiệm phối hợp với cơ quan chức năng có thẩm quyền trong ngăn chặn, phòng ngừa, xử lý hành vi vi phạm pháp luật của các doanh nghiệp cung cấp dịch vụ qua biên giới.

4. Mọi hành vi lợi dụng hoặc lạm dụng các biện pháp bảo vệ an ninh mạng để vi phạm pháp luật thì tùy theo tính chất, mức độ vi phạm mà bị xử lý theo quy định của pháp luật; trường hợp gây thiệt hại đến quyền và lợi ích hợp pháp của tổ chức, cá nhân thì phải bồi thường theo quy định của pháp luật.

5. Đối với các hệ thống thông tin không nằm trong Danh mục hệ thống thông tin quan trọng về an ninh quốc gia, Bộ Công an, Bộ Quốc phòng, Bộ Thông tin và Truyền thông phối hợp đồng bộ bảo vệ an ninh mạng, bảo đảm an toàn thông tin mạng theo chức năng, nhiệm vụ được giao:

a) Bộ Thông tin và Truyền thông là đầu mối chủ trì đối với các hoạt động dân sự, trừ trường hợp quy định tại điểm b, c khoản này;

b) Bộ Công an là đầu mối chủ trì đối với các hoạt động bảo vệ an ninh quốc gia, trật tự an toàn xã hội, bảo vệ an ninh mạng, phòng, chống tội phạm mạng, khủng bố mạng, gián điệp mạng;

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

Chương IV
TRIỂN KHAI MỘT SỐ HOẠT ĐỘNG BẢO VỆ AN NINH MẠNG TRONG CƠ QUAN NHÀ NƯỚC, TỔ CHỨC CHÍNH TRỊ Ở TRUNG ƯƠNG VÀ ĐỊA PHƯƠNG

Điều 23. Xây dựng, hoàn thiện quy định sử dụng mạng máy tính của cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương

1. Cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương phải xây dựng quy định sử dụng, quản lý và bảo đảm an ninh mạng máy tính nội bộ, mạng máy tính có kết nối mạng Internet do cơ quan, tổ chức mình quản lý. Nội dung các quy định về bảo đảm an toàn, an ninh mạng căn cứ vào những quy định về bảo vệ an ninh mạng, bảo vệ bí mật nhà nước, tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin mạng và các tiêu chuẩn kỹ thuật chuyên ngành khác có liên quan.

2. Quy định sử dụng, bảo đảm an ninh mạng máy tính của cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương phải bao gồm các nội dung cơ bản sau:

a) Xác định rõ hệ thống mạng thông tin và thông tin quan trọng cần ưu tiên bảo đảm an ninh mạng;

b) Quy định rõ các điều cấm và các nguyên tắc quản lý, sử dụng và bảo đảm an ninh mạng, mạng máy tính nội bộ có lưu trữ, truyền đưa bí mật nhà nước phải được tách biệt vật lý hoàn toàn với mạng máy tính, các thiết bị, phương tiện điện tử có kết nối mạng Internet, trường hợp khác phải bảo đảm quy định của pháp luật về bảo vệ bí mật nhà nước;

c) Quy trình quản lý, nghiệp vụ, kỹ thuật trong vận hành, sử dụng và bảo đảm an ninh mạng đối với dữ liệu, hạ tầng kỹ thuật, trong đó phải đáp ứng các yêu cầu cơ bản bảo đảm an toàn hệ thống thông tin;

d) Điều kiện về nhân sự làm công tác quản trị mạng, vận hành hệ thống, bảo đảm an ninh mạng, an toàn thông tin và liên quan đến hoạt động soạn thảo, lưu trữ, truyền đưa bí mật nhà nước qua hệ thống mạng máy tính;

đ) Quy định rõ trách nhiệm của từng bộ phận, cán bộ, nhân viên trong quản lý, sử dụng, bảo đảm an ninh mạng, an toàn thông tin;

e) Chế tài xử lý những vi phạm quy định về đảm bảo an ninh mạng.

Điều 24. Xây dựng, hoàn thiện phương án bảo đảm an ninh mạng đối với hệ thống thông tin của cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương

1. Người đứng đầu cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương có trách nhiệm ban hành phương án bảo đảm an ninh mạng đối với hệ thống thông tin do mình quản lý, bảo đảm đồng bộ, thống nhất, tập trung, có sự chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư trùng lặp.

2. Phương án bảo đảm an ninh mạng đối với hệ thống thông tin bao gồm:

a) Quy định bảo đảm an ninh mạng trong thiết kế, xây dựng hệ thống thông tin, đáp ứng yêu cầu cơ bản như yêu cầu quản lý, kỹ thuật, nghiệp vụ;

b) Thẩm định an ninh mạng;

c) Kiểm tra, đánh giá an ninh mạng;

d) Giám sát an ninh mạng;

đ) Dự phòng, ứng phó, khắc phục sự cố, tình huống nguy hiểm về an ninh mạng;

e) Quản lý rủi ro;

g) Kết thúc vận hành, khai thác, sửa chữa, thanh lý, hủy bỏ.

Điều 25. Phương án ứng phó, khắc phục sự cố an ninh mạng của cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương

1. Phương án ứng phó, khắc phục sự cố an ninh mạng bao gồm:

a) Phương án phòng ngừa, xử lý thông tin có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; làm nhục, vu khống; xâm phạm trật tự quản lý kinh tế bị đăng tải trên hệ thống thông tin;

b) Phương án 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;

c) Phương án 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;

d) Phương án phòng, chống tấn công mạng;

đ) Phương án phòng, chống khủng bố mạng;

e) Phương án phòng ngừa, xử lý tình huống nguy hiểm về an ninh mạng.

2. Nội dung phương án ứng phó, khắc phục sự cố an ninh mạng

a) Các quy định chung;

b) Đánh giá các nguy cơ, sự cố an ninh mạng;

c) Phương án ứng phó, khắc phục đối với một số tình huống cụ thể;

d) Nhiệm vụ, trách nhiệm của các cơ quan trong tổ chức, điều phối, xử lý, ứng phó, khắc phục sự cố;

đ) Huấn luyện, diễn tập, phòng ngừa sự cố, giám sát phát hiện, bảo đảm các điều kiện sẵn sàng đối phó, khắc phục sự cố;

e) Các giải pháp đảm bảo, tổ chức triển khai phương án, kế hoạch và kinh phí thực hiện.

Chương V
LƯU TRỮ DỮ LIỆU VÀ ĐẶT CHI NHÁNH HOẶC VĂN PHÒNG ĐẠI DIỆN TẠI VIỆT NAM

Điều 26. Lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam

1. Dữ liệu phải lưu trữ tại Việt Nam:

a) Dữ liệu về thông tin cá nhân của người sử dụng dịch vụ tại Việt Nam;

b) Dữ liệu do người sử dụng dịch vụ tại Việt Nam tạo ra: Tên tài khoản sử dụng dịch vụ, thời gian sử dụng dịch vụ, thông tin thẻ tín dụng, địa chỉ thư điện tử, địa chỉ mạng (IP) đăng nhập, đăng xuất gần nhất, số điện thoại đăng ký được gắn với tài khoản hoặc dữ liệu;

c) Dữ liệu về mối quan hệ của người sử dụng dịch vụ tại Việt Nam: bạn bè, nhóm mà người sử dụng kết nối hoặc tương tác.

2. Doanh nghiệp trong nước lưu trữ dữ liệu quy định tại khoản 1 Điều này tại Việt Nam.

3. Việc lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam của doanh nghiệp nước ngoài:

a) Doanh nghiệp nước ngoài có hoạt động kinh doanh tại Việt Nam thuộc một trong những lĩnh vực sau: Dịch vụ viễn thông; lưu trữ, chia sẻ dữ liệu trên không gian mạng; cung cấp tên miền quốc gia hoặc quốc tế cho người sử dụng dịch vụ tại Việt Nam; thương mại điện tử; thanh toán trực tuyến; trung gian thanh toán; dịch vụ kết nối vận chuyển qua không gian mạng; mạng xã hội và truyền thông xã hội; trò chơi điện tử trên mạng; dịch vụ cung cấp, quản lý hoặc vận hành thông tin khác trên không gian mạng dưới dạng tin nhắn, cuộc gọi thoại, cuộc gọi video, thư điện tử, trò chuyện trực tuyến phải lưu trữ dữ liệu quy định tại khoản 1 Điều này và đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam trong trường hợp dịch vụ do doanh nghiệp cung cấp bị sử dụng thực hiện hành vi vi phạm pháp luật về an ninh mạng đã được Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an thông báo và có yêu cầu phối hợp, ngăn chặn, điều tra, xử lý bằng văn bản nhưng không chấp hành, chấp hành không đầy đủ hoặc ngăn chặn, cản trở, vô hiệu hóa, làm mất tác dụng của biện pháp bảo vệ an ninh mạng do lực lượng chuyên trách bảo vệ an ninh mạng thực hiện;

b) Trường hợp bất khả kháng mà việc chấp hành yêu cầu của pháp luật về an ninh mạng của doanh nghiệp nước ngoài không thể thực hiện, doanh nghiệp nước ngoài thông báo cho Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an trong vòng 03 ngày làm việc để kiểm tra tính xác thực của việc bất khả kháng. Trong trường hợp này, doanh nghiệp có thời gian 30 ngày làm việc để tìm phương án khắc phục.

4. Trường hợp dữ liệu do doanh nghiệp thu thập, khai thác, phân tích, xử lý không đầy đủ theo quy định tại khoản 1 Điều này, doanh nghiệp phối hợp với Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an để xác nhận và tiến hành lưu trữ các loại dữ liệu hiện đang thu thập, khai thác, phân tích, xử lý.

Trường hợp doanh nghiệp tiến hành thu thập, khai thác, phân tích, xử lý bổ sung các loại dữ liệu theo quy định tại khoản 1 Điều này, doanh nghiệp có trách nhiệm phối hợp với Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an để bổ sung vào danh sách dữ liệu phải lưu trữ tại Việt Nam.

5. Hình thức lưu trữ dữ liệu tại Việt Nam do doanh nghiệp quyết định.

6. Trình tự, thủ tục yêu cầu lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện của doanh nghiệp nước ngoài tại Việt Nam:

a) Bộ trưởng Bộ Công an ra quyết định yêu cầu lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam;

b) Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an thông báo, hướng dẫn, theo dõi, giám sát, đôn đốc doanh nghiệp thực hiện yêu cầu lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam; đồng thời, thông báo cho các cơ quan liên quan để thực hiện chức năng quản lý nhà nước theo thẩm quyền;

c) Trong thời hạn 12 tháng kể từ ngày Bộ trưởng Bộ Công an ra quyết định, các doanh nghiệp quy định tại điểm a khoản 3 Điều 26 của Nghị định này phải hoàn thành lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam.

7. Trình tự, thủ tục đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam được thực hiện theo các quy định của pháp luật về kinh doanh, thương mại, doanh nghiệp và các quy định khác có liên quan.

8. Các doanh nghiệp không chấp hành quy định tại Điều này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý theo quy định của pháp luật.

Điều 27. Thời gian lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam

1. Thời gian lưu trữ dữ liệu theo quy định tại Điều 26 Nghị định này bắt đầu từ khi doanh nghiệp nhận được yêu cầu lưu trữ dữ liệu đến khi kết thúc yêu cầu. Thời gian lưu trữ tối thiểu là 24 tháng.

2. Thời gian đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam theo quy định tại Điều 26 Nghị định này bắt đầu từ khi doanh nghiệp nhận được yêu cầu đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam đến khi doanh nghiệp không còn hoạt động tại Việt Nam hoặc dịch vụ được quy định không còn cung cấp tại Việt Nam.

3. Nhật ký hệ thống để phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng được quy định tại điểm b khoản 2 Điều 26 của Luật An ninh mạng được lưu trữ tối thiểu là 12 tháng.

Chương VI
ĐIỀU KHOẢN THI HÀNH

Điều 28. Kinh phí bảo đảm

1. Kinh phí thực hiện bảo đảm an ninh mạng trong hoạt động của cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương do ngân sách nhà nước bảo đảm.

2. Kinh phí đầu tư cho an ninh mạng sử dụng vốn đầu tư công thực hiện theo quy định của Luật Đầu tư công. Đối với dự án đầu tư công để xây dựng mới hoặc mở rộng, nâng cấp hệ thống thông tin, kinh phí đầu tư được bố trí trong vốn đầu tư của dự án tương ứng.

3. Kinh phí thực hiện thẩm định, giám sát, kiểm tra, đánh giá điều kiện an ninh mạng; thực hiện các phương án bảo đảm an ninh mạng của cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương được cân đối, bố trí trong dự toán ngân sách hàng năm của cơ quan, tổ chức đó theo phân cấp của Luật Ngân sách nhà nước.

4. Bộ Tài chính hướng dẫn chi kinh phí phục vụ công tác bảo vệ an ninh mạng trong dự toán ngân sách, hướng dẫn quản lý và sử dụng kinh phí chi thường xuyên cho công tác bảo đảm an ninh mạng của cơ quan, tổ chức nhà nước.

5. Căn cứ nhiệm vụ được giao, cơ quan, tổ chức nhà nước thực hiện lập dự toán, quản lý, sử dụng và quyết toán kinh phí thực hiện nhiệm vụ bảo đảm an ninh mạng theo quy định của Luật Ngân sách nhà nước.

Điều 29. Hiệu lực thi hành

Nghị định này có hiệu lực từ ngày 01 tháng 10 năm 2022.

Điều 30. Trách nhiệm thi hành

1. Bộ trưởng Bộ Công an đôn đốc, kiểm tra, hướng dẫn việc thực hiện Nghị định này. Trong quá trình thực hiện, nếu có vướng mắc, các bộ, ngành, địa phương trao đổi Bộ Công an để tập hợp, báo cáo Chính phủ xem xét, quyết định, điều chỉnh.

2. Bộ trưởng, Thủ trưởng cơ quan ngang bộ, Thủ trưởng cơ quan thuộc Chính phủ, Chủ tịch Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương chịu trách nhiệm thi hành Nghị định này.

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

TM. CHÍNH PHỦ
KT. THỦ TƯỚNG
PHÓ THỦ TƯỚNG

Vũ Đức Đam

Phụ lục

(Kèm theo Nghị định số 53/2022/NĐ-CP ngày 15 tháng 8 năm 2022 của Chính phủ)

Mẫu số 01	Văn bản đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia
Mẫu số 02	Văn bản cung cấp danh mục toàn bộ hệ thống thông tin của cơ quan, tổ chức
Mẫu số 03	Văn bản phản hồi tiếp nhận Hồ sơ đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia
Mẫu số 04	Văn bản thông báo ý kiến của Hội đồng thẩm định đối với hồ sơ đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia
Mẫu số 05	Văn bản đề nghị đưa hệ thống thông tin ra khỏi Danh mục hệ thống thông tin quan trọng về an ninh quốc gia
Mẫu số 06	Văn bản thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia
Mẫu số 07	Văn bản đề nghị chứng nhận điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

Mẫu số 01

CƠ QUAN, TỔ CHỨC	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**
	Độc lập - Tự do - Hạnh phúc
Số: … V/v đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia	*....., ngày ... tháng ... năm ...*

Kính gửi: ……..[1].

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

Căn cứ Nghị định số …/2022/NĐ-CP ngày … tháng … năm … của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng;

…….[2] đề nghị đưa hệ thống thông tin sau vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia:

1. Hệ thống thông tin đề nghị đưa vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia

a) Thông tin chung

- Tên hệ thống thông tin:

- Địa chỉ (nơi đặt hệ thông tin):

- Người phụ trách (*họ tên, chức vụ, số điện thoại, địa chỉ thư điện tử*):

b) Phạm vi, quy mô của hệ thống thông tin

- Tầm quan trọng:

- Mục đích sử dụng:

- Đối tượng phục vụ của hệ thống thông tin:

- Yêu cầu bảo vệ an ninh mạng:

2. Đơn vị chủ quản hệ thống thông tin

- Tên đơn vị:

- Văn bản quyết định thành lập/quy định chức năng, nhiệm vụ, quyền hạn:

- Người đại diện:

- Địa chỉ:

- Thông tin liên hệ (*số điện thoại, địa chỉ thư điện tử*):

[1] Cơ quan thẩm định theo quy định tại khoản 1, khoản 2, khoản 3 Điều 5 của Nghị định này.
[2] Tên cơ quan, tổ chức.

3. Đơn vị vận hành hệ thống thông tin

- Tên đơn vị:

- Văn bản quyết định thành lập/quy định chức năng, nhiệm vụ, quyền hạn:

- Người đại diện:

- Địa chỉ:

- Thông tin liên hệ (*số điện thoại, địa chỉ thư điện tử*):

4. Thuyết minh chi tiết sự phù hợp với căn cứ xác lập hệ thống thông tin quan trọng về an ninh quốc gia

a) Sự phù hợp với quy định tại khoản 2 Điều 10 Luật An ninh mạng (*nêu rõ căn cứ, lập luận chứng minh và các văn bản có liên quan*)

b) Sự phù hợp với quy định về hệ thống thông tin quan trọng quốc gia, công trình quan trọng liên quan đến an ninh quốc gia, công trình viễn thông quan trọng liên quan đến an ninh quốc gia (*nêu rõ căn cứ, lập luận chứng minh và các văn bản có liên quan*):

c) Đánh giá phạm vi, mức độ ảnh hưởng và xác định hậu quả của 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 (*nêu rõ căn cứ, lập luận chứng minh và các văn bản có liên quan*).

5. Thuyết minh cấu trúc của hệ thống thông tin

a) Cấu trúc vật lý mô tả các thiết bị mạng, các thiết bị đầu cuối có trong hệ thống và kết nối vật lý giữa các thiết bị (*sơ đồ kết nối vật lý*).

b) Cấu trúc logic mô tả thiết kế các vùng mạng chức năng có trong hệ thống; hướng hết nối mạng; các thiết bị đầu cuối; các thiết bị mạng (*sơ đồ kết nối logic*).

c) Danh mục thiết bị sử dụng trong hệ thống (*thông tin tên thiết bị/chủng loại; vị trí triển khai, trường hợp thiết bị vật lý được chia thành các thiết bị logic thì vị trí triển khai là các vị trí của thiết bị logic; mục đích sử dụng*).

d) Danh mục các ứng dụng, dịch vụ trên hệ thống (*tên ứng dụng, dịch vụ; tên và cấu hình máy chủ/vị trí triển khai/hệ điều hành; mục đích sử dụng*).

đ) Danh mục đề xuất các thành phần, thiết bị mạng và mức độ quan trọng cần ưu tiên bảo vệ (*tên thiết bị, thông tin xử lý, chức năng/mức độ quan trọng*).

6. Thuyết minh phương án bảo đảm an ninh mạng về quản lý và kỹ thuật

a) Phương án bảo đảm an ninh mạng về quản lý (*nêu rõ phương án đã ban hành hoặc dự kiến ban hành, nội dung cơ bản, mục tiêu bảo vệ*).

b) Phương án bảo đảm an ninh mạng về kỹ thuật (*nêu rõ phương án đã ban hành hoặc dự kiến ban hành, nội dung cơ bản, mục tiêu bảo vệ*)

c) Phương án bảo đảm an ninh mạng về ứng phó, khắc phục sự cố an ninh mạng (*nêu rõ phương án đã ban hành hoặc dự kiến ban hành, nội dung cơ bản, mục tiêu bảo vệ*).

7. Tài liệu kèm theo

a) Danh mục thống kê toàn bộ hệ thống thông tin của cơ quan, tổ chức (*tên hệ thống thông tin, chức năng của hệ thống thông tin, mục đích sử dụng*).

b) Tài liệu thiết kế thi công đã được cấp có thẩm quyền phê duyệt hoặc tài liệu có giá trị tương đương (*trường hợp không có tài liệu thiết kế thi công, cần nêu rõ lý do*).

c) Các tài liệu khác là căn cứ được trích dẫn, nêu trong công văn này.

Nơi nhận:
- Như trên;
- ……..

ĐẠI DIỆN CƠ QUAN, TỔ CHỨC
(Ký, ghi rõ họ tên, chức danh và đóng dấu)

Mẫu số 02

CƠ QUAN, TỔ CHỨC	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**
	Độc lập - Tự do - Hạnh phúc
Số: …	*....., ngày ... tháng ... năm ...*
V/v cung cấp danh mục toàn bộ hệ thống thông tin	

Kính gửi: ……..[1]

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

Căn cứ Nghị định số …/2022/NĐ-CP ngày … tháng … năm … của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng;

…..[2] cung cấp danh mục toàn bộ hệ thống thông tin hiện có như sau:

STT	Tên hệ thống thông tin	Đơn vị chủ quản	Địa chỉ	Thông tin liên hệ
1	Hệ thống thông tin A	- Tên đơn vị:		Người phụ trách (*họ tên, chức vụ, số điện thoại, địa chỉ thư điện tử*)

Nơi nhận:
- Như trên;
- ……..

ĐẠI DIỆN CƠ QUAN, TỔ CHỨC
(Ký, ghi rõ họ tên, chức danh và đóng dấu)

[1] Cơ quan thẩm định theo quy định tại khoản 1, khoản 2, khoản 3 Điều 5 của Nghị định này.
[2] Tên cơ quan, đơn vị.

Mẫu số 03

CƠ QUAN, TỔ CHỨC[1]	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**
	Độc lập - Tự do - Hạnh phúc
Số: ……..	*….., ngày ... tháng ... năm ...*
V/v tiếp nhận hồ sơ đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia	

Kính gửi: ……[2]

….[3] nhận được công văn số ….. ngày ….. tháng ..... năm ….. của ….[4] về việc đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia, như sau:

1. Thời gian nhận Hồ sơ đề nghị (*ghi rõ giờ, ngày, tháng, năm*):

……

2. Hồ sơ đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia, gồm: …

……

……

Đề nghị bổ sung (*trường hợp hồ sơ chưa đầy đủ*):

……

……

Thời hạn bổ sung (*ghi ngày, tháng, năm*):

……

3. Thời gian phản hồi ý kiến: dự kiến … giờ… ngày… tháng… năm…

Nơi nhận:	**ĐẠI DIỆN CƠ QUAN, TỔ CHỨC**
- Như trên;	*(Ký, ghi rõ họ tên, chức danh và đóng dấu)*
- ……..	

[1] Cơ quan thẩm định theo quy định tại khoản 1, khoản 2, khoản 3 Điều 5 của Nghị định này.
[2] Cơ quan, đơn vị gửi hồ sơ đề nghị.
[3] Cơ quan tiếp nhận hồ sơ (cơ quan thẩm định theo quy định tại khoản 1, khoản 2, khoản 3 Điều 5 của Nghị định này).
[4] Cơ quan, đơn vị gửi hồ sơ đề nghị.

Mẫu số 04

CƠ QUAN, TỔ CHỨC[1]	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**
	Độc lập - Tự do - Hạnh phúc
Số: ……..	*....., ngày ... tháng ... năm ...*
V/v thông báo ý kiến của Hội đồng thẩm định đối với hồ sơ đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia	

Kính gửi: ……[2]

Ngày … tháng … năm …, Hội đồng thẩm định đã họp, cho ý kiến đối với Hồ sơ đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia của ….[3], như sau:

1. Kết quả phiếu lấy ý kiến

STT	Tên hệ thống thông tin	Kết quả	
		Đạt	Chưa đạt
1		/	/

2. Kết luận

……

……

3. Đề nghị:

……

……

Nơi nhận:
- Như trên;
- ……..

ĐẠI DIỆN CƠ QUAN, TỔ CHỨC
(Ký, ghi rõ họ tên, chức danh và đóng dấu)

[1] Cơ quan thẩm định theo quy định tại khoản 1, khoản 2, khoản 3 Điều 5 của Nghị định này.
[2] Cơ quan, đơn vị gửi hồ sơ đề nghị.
[3] Cơ quan, đơn vị gửi hồ sơ đề nghị.

Mẫu số 05

CƠ QUAN, TỔ CHỨC	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**
	Độc lập - Tự do - Hạnh phúc
Số: ……..	*....., ngày ... tháng ... năm ...*
V/v đề nghị đưa hệ thống thông tin ra khỏi Danh mục hệ thống thông tin quan trọng về an ninh quốc gia	

Kính gửi: ……[1]

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

Căn cứ Nghị định số .../2022/NĐ-CP ngày … tháng … năm … của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng;

….[2] đề nghị đưa hệ thống thông tin sau ra khỏi Danh mục hệ thống thông tin quan trọng về an ninh quốc gia:

1. Thông tin chung

- Tên hệ thống thông tin: …

- Đơn vị chủ quản hệ thống thông tin: …

- Địa chỉ: …

- Quyết định đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia (*nêu rõ số, ngày tháng, trích yếu văn bản*):

2. Lý do

……

3. Tài liệu kèm theo (*tài liệu chứng minh hệ thống thông tin không còn phù hợp là hệ thống thông tin quan trọng về an ninh quốc gia*)

……

Nơi nhận:	**ĐẠI DIỆN CƠ QUAN, TỔ CHỨC**
- Như trên;	*(Ký, ghi rõ họ tên, chức danh và đóng dấu)*
- ……..	

[1] Cơ quan thẩm định theo quy định tại khoản 1, khoản 2, khoản 3 Điều 5 của Nghị định này.

[2] Tên cơ quan, đơn vị.

Mẫu số 06

CƠ QUAN, TỔ CHỨC	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**
	Độc lập - Tự do - Hạnh phúc
Số: …….. V/v thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia	*….., ngày ... tháng ... năm ...*

Kính gửi: ……..[1]

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

Căn cứ Nghị định số .../2022/NĐ-CP ngày ... tháng ... năm ... của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng;

……..[2] đề nghị thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia:

1. Thông tin chung:

- Tên hệ thống thông tin: ...

- Đơn vị chủ quản hệ thống thông tin: ...

- Địa chỉ: ...

- Quyết định đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia (*nêu rõ số, ngày tháng, trích yếu văn bản*):

2. Tài liệu kèm theo:

a) Báo cáo nghiên cứu tiền khả thi, hồ sơ thiết kế thi công dự án đầu tư xây dựng hệ thống thông tin trước khi phê duyệt;

b) Đề án nâng cấp hệ thống thông tin trước khi phê duyệt trong trường hợp nâng cấp hệ thống thông tin quan trọng về an ninh quốc gia.

Nơi nhận: - Như trên; - ……..	**ĐẠI DIỆN CƠ QUAN, TỔ CHỨC** *(Ký, ghi rõ họ tên, chức danh và đóng dấu)*

[1] Cơ quan thẩm định theo quy định tại khoản 1, khoản 2, khoản 3 Điều 5 của Nghị định này.
[2] Tên cơ quan, đơn vị.

Mẫu số 07

CƠ QUAN, TỔ CHỨC	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**
	Độc lập - Tự do - Hạnh phúc
Số: …….. V/v đề nghị chứng nhận điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia	*….., ngày ... tháng ... năm ...*

Kính gửi: ……..[1]

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

Căn cứ Nghị định số …/2022/NĐ-CP ngày … tháng … năm … của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng;

……..[2] đề nghị chứng nhận điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia:

1. Thông tin chung:

- Tên hệ thống thông tin: …

- Đơn vị chủ quản hệ thống thông tin: …

- Địa chỉ: …

- Quyết định đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia (*nêu rõ số, ngày tháng, trích yếu văn bản*):

2. Tài liệu kèm theo:

a) Báo cáo nghiên cứu tiền khả thi, hồ sơ thiết kế thi công dự án đầu tư xây dựng hệ thống thông tin trước khi phê duyệt;

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

Nơi nhận: - Như trên; - ……..	**ĐẠI DIỆN CƠ QUAN, TỔ CHỨC** *(Ký, ghi rõ họ tên, chức danh và đóng dấu)*

[1] Cơ quan thẩm định theo quy định tại khoản 1, khoản 2, khoản 3 Điều 5 của Nghị định này.
[2] Tên cơ quan, đơn vị.