BỘ KẾ HOẠCH VÀ ĐẦU TƯ

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

Số: 1709 /QĐ-BKHĐT

Hà Nội, ngày 24 tháng 12 năm 2021

QUYẾT ĐỊNH
Ban hành Quy chế bảo đảm an toàn thông tin, an ninh mạng máy tính của Bộ Kế hoạch và Đầu tư

BỘ TRƯỞNG BỘ KẾ HOẠCH VÀ ĐẦU TƯ

Căn cứ Luật Công nghệ thông tin ngày 29 tháng 6 năm 2006;

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

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

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Nghị định số 86/2017/NĐ-CP ngày 25 tháng 7 năm 2017 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Kế hoạch và Đầu tư;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ ban hành Quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Căn cứ Chỉ thị số 14/CT-TTg ngày 25 tháng 5 năm 2018 của Thủ tướng Chính phủ về việc nâng cao năng lực phòng, chống phần mềm độc hại;

Căn cứ Chỉ thị số 14/TC-TTg ngày 07 tháng 6 năm 2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam;

Căn cứ Thông tư số 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;

Căn cứ Thông tư số 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin;

Theo đề nghị của Giám đốc Trung tâm Tin học.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn thông tin, an ninh mạng máy tính Bộ Kế hoạch và Đầu tư.

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày ký và thay thế Quyết định số 1180/QĐ-BKHĐT ngày 24 tháng 8 năm 2015 của Bộ trưởng Bộ Kế hoạch và Đầu tư.

Điều 3. Giám đốc Trung tâm Tin học, Chánh Văn phòng Bộ, Thủ trưởng các đơn vị thuộc Bộ chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Bộ trưởng;
- Các Thứ trưởng;
- Đảng ủy, Công đoàn cơ quan;
- Lưu: VT, TTTH (02b).

BỘ TRƯỞNG

BỘ KẾ HOẠCH VÀ ĐẦU TƯ

Nguyễn Chí Dũng

BỘ KẾ HOẠCH VÀ ĐẦU TƯ

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

QUY CHẾ
Bảo đảm an toàn thông tin, an ninh mạng máy tính của Bộ Kế hoạch và Đầu tư

(Ban hành kèm theo Quyết định số 1709 /QĐ-BKHĐT ngày 24 tháng 12 năm 2021 của Bộ trưởng Bộ Kế hoạch và Đầu tư)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. Phạm vi điều chỉnh: Quy chế này quy định về bảo đảm an toàn thông tin, an ninh mạng trong ứng dụng công nghệ thông tin, chuyển đổi số của Bộ Kế hoạch và Đầu tư.

2. Đối tượng áp dụng: Quy chế này được áp dụng với các đơn vị, tổ chức, cá nhân liên quan đến việc ứng dụng công nghệ thông tin, chuyển đổi số của Bộ Kế hoạch và Đầu tư.

Điều 2. Giải thích từ ngữ

1. *"Đơn vị chuyên trách về an toàn thông tin, an ninh mạng"* là đơn vị thực hiện chức năng, nhiệm vụ của: Đơn vị chuyên trách về an toàn thông tin (theo quy định tại Khoản 5, Điều 3 Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ quy định về bảo đảm an toàn hệ thống thông tin theo cấp độ); Đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng (theo quy định tại Điều 6 Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia); Lực lượng bảo vệ an ninh mạng (quy định tại Điều 30 Luật An ninh mạng năm 2018).

2. *"Đơn vị quản lý, vận hành hệ thống thông tin"* là tổ chức, đơn vị được giao quản lý vận hành trực tiếp đối với hệ thống thông tin.

3. *"WPA2-Enterprise"* là kiểu xác thực mạng không dây, sử dụng tên và mật khẩu để đăng nhập.

4. *"Mật khẩu mạnh"* là một chuỗi có tối thiểu 8 ký tự, bao gồm chữ thường, chữ in hoa, ký tự đặc biệt và được thay đổi định kỳ chậm nhất 90 ngày sử dụng.

Điều 3. Nguyên tắc chung

1. Bảo đảm an toàn thông tin, an ninh mạng là yêu cầu bắt buộc, thường xuyên, liên tục, xuyên suốt quá trình thiết kế, xây dựng, quản lý vận hành, nâng

cấp, hủy bỏ hệ thống thông tin. Thực hiện nghiêm theo quy định của pháp luật có liên quan và Quy chế này.

2. Xử lý sự cố an toàn thông tin, an ninh mạng phải phù hợp với trách nhiệm, quyền hạn và bảo đảm lợi ích hợp pháp của cơ quan, đơn vị, cá nhân liên quan và theo quy định của pháp luật.

Điều 4. Các hành vi bị nghiêm cấm

1. Thực hiện quy định tại Điều 12 Luật Công nghệ thông tin, Điều 7 Luật An toàn thông tin mạng và Điều 8 Luật An ninh mạng.

2. Cung cấp, đăng tải, truyền đưa thông tin có nội dung quy định tại các khoản 1, 2, 3, 4 và 5 Điều 16 của Luật An ninh mạng năm 2018 và thông tin khác có nội dung xâm phạm an ninh quốc gia trên Trang thông tin điện tử, cổng thông tin điện tử hoặc chuyên trang trên mạng xã hội của đơn vị, tổ chức, cá nhân.

CHƯƠNG II
QUY ĐỊNH CỤ THỂ

Điều 5. Bảo đảm an toàn thông tin, an ninh mạng đối với hệ thống mạng

1. Hệ thống mạng nội bộ (LAN) phải được thiết kế phân vùng theo chức năng cơ bản, bao gồm: vùng mạng người dùng; vùng mạng kết nối hệ thống ra bên ngoài Internet và các mạng khác; vùng mạng máy chủ công cộng; vùng mạng máy chủ nội bộ; vùng mạng máy chủ cơ sở dữ liệu, vùng mạng máy chủ quản trị. Dữ liệu trao đổi giữa các vùng mạng phải được quản lý, giám sát bởi hệ thống các thiết bị mạng, thiết bị bảo mật.

2. Máy tính kết nối mạng.

a) Phải được cài đặt phần mềm có bản quyền hoặc phần mềm mã nguồn mở thuộc danh mục do Bộ Thông tin và Truyền thông ban hành đồng thời phải được thiết lập phương thức xác thực an toàn.

b) Phải được cài đặt phần mềm phòng chống mã độc tập trung do đơn vị chuyên trách về an toàn thông tin, an ninh mạng triển khai.

c) Phải đặt tên máy tính theo quy ước: [Viết tắt tên Người sử dụng] + [Số phòng] + [Tên tòa nhà]; Tên nhóm: đặt tên nhóm theo tên viết tắt của đơn vị.

d) Phải được cấu hình nhằm vô hiệu hóa tính năng tự động thực thi (autoplay) các tệp tin trên các thiết bị lưu trữ di động.

3. Thiết bị phát sóng và kết nối mạng không dây phải hỗ trợ kiểu xác thực WPA2-Enterprise. Mọi đối tượng quy định tại Điều 1 khi kết nối mạng không dây phải sử dụng tài khoản truy cập được cấp. Khách đến làm việc tại Bộ chỉ được kết

nối mạng không dây để truy cập Internet và sử dụng thông tin xác thực do đơn vị quản lý, vận hành hệ thống thông tin cung cấp.

4. Hệ thống mạng do các đơn vị thuộc Bộ được giao quản lý, vận hành phải được kết nối mạng nội bộ với Trung tâm dữ liệu của Bộ để triển khai việc chia sẻ thông tin, dữ liệu và giám sát an toàn thông tin theo quy định.

Điều 6. Bảo đảm an toàn thông tin, an ninh mạng tại Trung tâm dữ liệu

1. Các thiết bị kết nối mạng, thiết bị bảo mật quan trọng như tường lửa, thiết bị định tuyến, hệ thống máy chủ, hệ thống lưu trữ... phải được đặt trong Trung tâm dữ liệu và phải được thiết lập cơ chế bảo vệ, theo dõi phát hiện xâm nhập và biện pháp kiểm soát truy cập, kết nối vật lý phù hợp với từng khu vực: máy chủ và hệ thống lưu trữ; tủ mạng và đầu nối; thiết bị nguồn điện và dự phòng điện khẩn cấp; vận hành, kiểm soát, quản trị hệ thống.

2. Trung tâm dữ liệu phải đáp ứng Tiêu chuẩn quốc gia TCVN 9250:2021 về Trung tâm dữ liệu - yêu cầu hạ tầng kỹ thuật viễn thông, có hệ thống điện dự phòng đủ công suất và duy trì thời gian hoạt động của các máy chủ ít nhất 24 giờ khi có sự cố mất điện; hệ thống làm mát điều hòa không khí, độ ẩm để bảo đảm môi trường vận hành; hệ thống cảnh báo cháy, hệ thống chữa cháy tự động, thiết bị phòng cháy, chữa cháy khẩn cấp; hệ thống cảnh báo hệ thống nguồn điện; hệ thống chống sét lan truyền. Các hệ thống này phải được thiết lập chế độ cảnh báo phù hợp.

3. Chỉ những cá nhân có quyền, nhiệm vụ theo quy định của thủ trưởng đơn vị được giao quản lý Trung tâm dữ liệu mới được phép vào, ra Trung tâm dữ liệu. Việc vào, ra Trung tâm dữ liệu phải được kiểm soát bằng thiết bị bảo vệ (quẹt thẻ, vân tay, sinh trắc học, ...).

4. Đối với phần mềm thương mại tại Trung tâm dữ liệu yêu cầu phải có bản quyền.

5. Toàn bộ thiết bị trong Trung tâm dữ liệu phải được lắp đặt, cài đặt, cấu hình đúng tiêu chuẩn chung của Trung tâm dữ liệu, được bảo trì, bảo dưỡng định kỳ để bảo đảm tính ổn định, sẵn sàng, an toàn trong vận hành. Tủ thiết bị của Trung tâm dữ liệu phải được khóa trừ thời gian thực hiện công việc.

6. Các vùng mạng, máy chủ trong Trung tâm dữ liệu phải được kiểm soát bởi tường lửa, các thiết bị, phầm mềm bảo mật. Mọi truy cập vào ra giữa các vùng mạng, máy chủ phải có hệ thống theo dõi, giám sát và phát hiện xâm nhập.

7. Các máy chủ phải được cài đặt phần mềm phòng chống mã độc và được quản lý thống nhất, tập trung.

8. Nhật ký hoạt động của thiết bị, phần mềm an toàn thông tin, an ninh mạng phải được lưu giữ tối thiểu 03 tháng để phục vụ công tác khảo sát, phân tích hoặc điều tra khi có sự cố xảy ra.

9. Quản lý việc mang thiết bị vào, ra Trung tâm dữ liệu

a) Việc mang thiết bị vào, ra để lắp đặt hoặc sửa chữa phải có sự đồng ý của Lãnh đạo đơn vị quản lý, vận hành.

b) Thời gian tháo lắp thiết bị thực hiện ngoài giờ hành chính trừ trường hợp xử lý sự cố khẩn cấp, trước khi vào Trung tâm dữ liệu thiết bị phải được bóc, dỡ vỏ, hộp.

10. Làm việc trong Trung tâm dữ liệu

a) Quá trình vào, ra Trung tâm dữ liệu phải được ghi vào sổ nhật ký.

b) Dữ liệu của hệ thống camera giám sát vào, ra phải lưu tối thiểu 03 tháng.

Điều 7. Bảo đảm an toàn thông tin, an ninh mạng đối với việc xây dựng, nâng cấp và sử dụng phần mềm ứng dụng

1. Yêu cầu về bảo đảm an toàn thông tin, an ninh mạng phải được đưa vào tất cả các công đoạn thiết kế, xây dựng, triển khai và vận hành, sử dụng phần mềm ứng dụng.

2. Phần mềm ứng dụng phải đáp ứng các yêu cầu sau: cấu hình phần mềm, ứng dụng để xác thực người sử dụng; giới hạn số lần đăng nhập sai liên tiếp; giới hạn thời gian để chờ đóng phiên kết nối; mã hóa thông tin xác thực trên hệ thống; không được để chế độ đăng nhập tự động.

3. Phần mềm ứng dụng cần được kiểm tra phát hiện và khắc phục các điểm yếu về an toàn thông tin, an ninh mạng trước khi đưa vào sử dụng và trong quá trình sử dụng.

4. Cá nhân sử dụng phần mềm do đơn vị quản lý, vận hành hệ thống mạng cung cấp, cài đặt hoặc hướng dẫn.

5. Thiết lập, phân quyền truy cập, quản trị, sử dụng tài nguyên khác nhau của phần mềm ứng dụng với người sử dụng/nhóm người sử dụng có chức năng, yêu cầu nghiệp vụ khác nhau; tách biệt cổng giao tiếp quản trị phần mềm ứng dụng với cổng giao tiếp cung cấp dịch vụ; đóng các cổng giao tiếp không sử dụng.

6. Chỉ cho phép sử dụng các giao thức mạng có hỗ trợ chức năng mã hóa thông tin (SSH, TSL, VPN hoặc tương đương) khi truy cập, quản trị phần mềm, ứng dụng từ xa trên môi trường mạng; hạn chế truy cập đến mã nguồn của phần mềm ứng dụng và phải đặt mã nguồn trong môi trường an toàn do bộ phận quản lý, vận hành hệ thống quản lý.

7. Các ứng dụng dùng chung, hệ thống thông tin, cơ sở dữ liệu trước khi nâng cấp, sửa chữa, bảo trì, xử lý sự cố phải thực hiện sao lưu.

8. Thực hiện quy trình kiểm soát cài đặt, cập nhật, vá lỗi bảo mật phần mềm, ứng dụng trên các máy chủ, máy tính cá nhân, thiết bị kết nối mạng đang hoạt động thuộc hệ thống mạng nội bộ.

Điều 8. Bảo đảm an toàn thông tin, an ninh mạng đối với dữ liệu

1. Đơn vị quản lý, vận hành hệ thống thông tin phải thiết lập phương án bảo đảm tính bí mật, nguyên vẹn và khả dụng của thông tin, dữ liệu; mã hóa thông tin, dữ liệu khi lưu trữ trên hệ thống/thiết bị lưu trữ dữ liệu di động; sử dụng chữ ký số để xác thực và bảo mật thông tin, dữ liệu.

2. Tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ phải được sao lưu dự phòng định kỳ và lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng.

3. Mỗi đơn vị cần bố trí máy tính, máy in riêng không kết nối mạng, đặt mật khẩu mạnh cho máy tính và tệp văn bản điện tử, mã hóa dữ liệu và các biện pháp bảo mật khác bảo đảm an toàn thông tin, an ninh mạng để soạn thảo, lưu trữ tài liệu mật.

4. Việc chia sẻ, gửi, nhận thông tin không công khai trên môi trường mạng phải sử dụng mật khẩu mạnh và mã hóa kết nối để bảo vệ thông tin.

Điều 9. Bảo đảm an toàn thông tin, an ninh mạng khi tiếp nhận, phát triển, vận hành và bảo trì hệ thống thông tin

1. Khi thực hiện nâng cấp, mở rộng, thay thế một phần hệ thống thông tin, đơn vị vận hành hệ thống thông tin phải rà soát cấp độ, phương án bảo đảm an toàn của hệ thống thông tin và thực hiện điều chỉnh, bổ sung hoặc thay mới hồ sơ đề xuất cấp độ trong trường hợp cần thiết.

2. Khi tiếp nhận, phát triển, nâng cấp, bảo trì hệ thống thông tin, đơn vị vận hành hệ thống thông tin phải tiến hành phân tích, xác định rủi ro có thể xảy ra, đánh giá phạm vi tác động và phải chuẩn bị các biện pháp hạn chế, loại trừ các rủi ro này và yêu cầu các bên cung cấp, thi công, các cá nhân liên quan thực hiện.

3. Trong quá trình vận hành hệ thống thông tin, đơn vị vận hành hệ thống thông tin cần thực hiện đánh giá, phân loại hệ thống thông tin theo cấp độ; triển khai phương án bảo đảm an toàn hệ thống thông tin đáp ứng yêu cầu cơ bản trong tiêu chuẩn, quy chuẩn kỹ thuật về bảo đảm an toàn hệ thống thông tin theo cấp độ; thường xuyên kiểm tra, giám sát an toàn hệ thống thông tin; tuân thủ quy trình vận hành, quy trình xử lý sự cố đã xây dựng; ghi lại và lưu trữ đầy đủ thông tin nhật ký hệ thống để phục vụ quản lý, kiểm soát thông tin.

4. Đơn vị vận hành hệ thống thông tin phải thực hiện công tác bảo đảm an toàn thông tin, an ninh mạng, tránh lộ, lọt mã nguồn và dữ liệu, tài liệu thiết kế, quản trị hệ thống mà đối tác đang xử lý ra bên ngoài khi xây dựng, nâng cấp.

Điều 10. Bảo đảm an toàn thông tin, an ninh mạng Trung tâm điều hành

1. Trung tâm điều hành phải được trang bị các hệ thống giám sát hoạt động liên tục, thông tin giám sát hoạt động được lưu tối thiểu 03 tháng.

2. Trung tâm điều hành phải có hệ thống điện dự phòng, hệ thống chống cháy và hệ thống chống sét; được trang bị hệ thống lưu điện đủ công suất và duy trì thời gian hoạt động của các thiết bị ít nhất 30 phút khi có sự cố mất điện.

3. Toàn bộ thiết bị trong Trung tâm điều hành phải được lắp đặt, cài đặt, cấu hình đúng thiết kế; được bảo trì, bảo dưỡng định kỳ để bảo đảm tính ổn định, sẵn sàng, an toàn trong vận hành.

4. Kết nối mạng từ Trung tâm điều hành về Trung tâm dữ liệu phải được mã hóa.

5. Thiết bị được lắp đặt cố định hay tạm thời tại Trung tâm điều hành phải được kiểm tra, giám sát bởi đơn vị chuyên trách về an toàn thông tin, an ninh mạng.

6. Chỉ được thực hiện ghi âm, ghi hình cuộc họp khi được sự đồng ý của người chủ trì cuộc họp.

Điều 11. Quản lý tài khoản truy cập

1. Mỗi cá nhân, đơn vị thuộc Bộ được cấp một tài khoản truy cập dùng chung cho mọi ứng dụng nội bộ của Bộ từ Hệ thống định danh tập trung, tài khoản truy cập với định danh duy nhất gắn với cá nhân đó, đơn vị đó chỉ truy cập vào các trang/cổng thông tin điện tử, ứng dụng trực tuyến và các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình. Thông tin tài khoản đăng nhập phải được ứng dụng kỹ thuật mã hóa và đặt mật khẩu mạnh.

2. Tài khoản quản trị hệ thống (mạng máy tính, hệ điều hành, thiết bị kết nối mạng, phần mềm, ứng dụng, cơ sở dữ liệu, hệ thống thông tin) phải tách biệt với tài khoản truy cập của người sử dụng thông thường. Tài khoản hệ thống phải được giao đích danh cá nhân làm công tác quản trị.

3. Đơn vị chuyên trách về an toàn thông tin, an ninh mạng cấp, khóa quyền truy cập của tài khoản các hệ thống thông tin trong trường hợp tài khoản đó thực hiện các hành vi tấn công hoặc để xảy ra vấn đề mất an toàn thông tin, an ninh mạng.

4. Trường hợp cá nhân thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ hưu, trong vòng không quá 05 ngày làm việc sau khi có quyết định của cấp có thẩm quyền thì cơ quan, đơn vị quản lý cá nhân đó phải thông báo cơ quan, đơn vị chuyên trách về an toàn thông tin, an ninh mạng để điều chỉnh, thu hồi, hủy bỏ các quyền sử dụng đối với hệ thống thông tin.

Điều 12. Giám sát an toàn thông tin, an ninh mạng

1. Thành phần giám sát trung tâm của đơn vị vận hành hệ thống thông tin cần đáp ứng các yêu cầu sau:

a) Cung cấp đầy đủ các tính năng thu thập và tổng hợp các thông tin an toàn thông tin mạng; phân tích các thông tin thu thập để phát hiện và cảnh báo tấn công, rủi ro, sự cố an toàn thông tin mạng có khả năng ảnh hưởng tới hoạt động hệ thống hoặc khả năng cung cấp các dịch vụ của hệ thống thông tin được giám sát; cung cấp giao diện thuận tiện cho việc theo dõi, giám sát liên tục của cán bộ giám sát.

b) Thực hiện thu thập và phân tích các thông tin đầu vào tối thiểu sau đây: nhật ký máy chủ web (web server) với các ứng dụng web (ví dụ: cổng thông tin điện tử, dịch vụ công trực tuyến v.v...); cảnh báo/nhật ký của thiết bị quan trắc cơ sở; cảnh báo/nhật ký của thiết bị tường lửa được thiết lập bảo vệ luồng kết nối mạng Internet liên quan đến các đối tượng cần giám sát.

c) Năng lực xử lý thành phần giám sát trung tâm của đơn vị vận hành hệ thống thông tin cần phù hợp với khối lượng, định dạng và có khả năng phân tích thông tin an toàn thông tin mạng thu thập từ các hệ thống được giám sát.

2. Thu thập thông tin an toàn thông tin mạng và quan trắc cơ sở cần đáp ứng các yêu cầu sau:

a) Thực hiện thu thập thông tin an toàn thông tin mạng từ nhật ký và cảnh báo của các phần mềm/thiết bị liên quan đến đối tượng cần giám sát để cung cấp cho thành phần giám sát trung tâm của đơn vị vận hành hệ thống thông tin hoặc theo yêu cầu của đơn vị chuyên trách về an toàn thông tin, an ninh mạng. Các thông tin tối thiểu cần thu thập và cung cấp bao gồm: nhật ký máy chủ web (web server) của các ứng dụng web (ví dụ: cổng thông tin điện tử, dịch vụ công trực tuyến v.v...); cảnh báo/nhật ký của thiết bị quan trắc cơ sở; cảnh báo/nhật ký của thiết bị tường lửa được thiết lập bảo vệ luồng kết nối mạng Internet liên quan đến các đối tượng cần giám sát.

b) Các thiết bị quan trắc cơ sở đảm bảo các chức năng phát hiện tấn công, rủi ro, sự cố an toàn thông tin mạng; cần được thiết lập để đảm bảo khả năng giám sát bao phủ được tất cả các đường kết nối mạng Internet của đối tượng cần giám sát.

c) Thiết bị quan trắc cần đáp ứng tối thiểu các chức năng phát hiện, tạo lập luật phát hiện tấn công riêng dựa trên các thông tin như: địa chỉ IP nguồn, địa chỉ IP đích, địa chỉ cổng nguồn, địa chỉ cổng đích, các đoạn dữ liệu đặc biệt trong gói tin được truyền qua.

d) Đối với các hệ thống thông tin phục vụ Chính phủ điện tử sử dụng giao thức có mã hóa (ví dụ: https), cần có phương án kỹ thuật đảm bảo thiết bị quan trắc an toàn thông tin mạng có được đầy đủ thông tin để có thể phát hiện được các tấn công, rủi ro, sự cố an toàn thông tin mạng.

e) Thiết lập, kết nối các thiết bị quan trắc cơ sở với hệ thống giám sát của Bộ Kế hoạch và Đầu tư và yêu cầu của đơn vị chuyên trách về đảm bảo an toàn thông tin, an ninh mạng.

3. Nội dung thực hiện giám sát:

a) Theo dõi, trực giám sát liên tục, lập báo cáo hằng ngày, đảm bảo hệ thống giám sát của đơn vị vận hành hệ thống thông tin hoạt động và thu thập thông tin ổn định, liên tục.

b) Theo dõi, vận hành các thiết bị quan trắc cơ sở đảm bảo ổn định, liên tục, điều chỉnh kịp thời khi có các thay đổi và thực hiện đầy đủ các hướng dẫn của Bộ Thông tin và Truyền thông để đảm bảo hiệu quả giám sát.

c) Lập báo cáo kết quả giám sát hằng tuần để báo cáo đơn vị vận hành hệ thống thông tin, nội dung báo cáo tuần bao gồm đầy đủ các thông tin sau: thời gian giám sát; danh mục đối tượng bị tấn công cần chú ý (địa chỉ IP, mô tả dịch vụ cung cấp, thời điểm bị tấn công); kỹ thuật tấn công đã phát hiện được và chứng cứ liên quan; các đối tượng thực hiện tấn công; các thay đổi trong hệ thống được giám sát và hệ thống giám sát; v.v....

d) Tiến hành phân loại nguy cơ, rủi ro, sự cố an toàn thông tin mạng tùy theo tình hình cụ thể.

e) Định kỳ thống kê kết quả xử lý nguy cơ, rủi ro, sự cố an toàn thông tin mạng để phục vụ công tác lưu trữ, báo cáo.

f) Trong trường hợp đơn vị vận hành hệ thống thông tin đề nghị đơn vị chuyên trách an toàn thông tin, an ninh mạng thực hiện giám sát cơ sở đơn vị vận hành hệ thống thông tin có trách nhiệm cung cấp và cập nhật thông tin về hệ thống thông tin cần giám sát và mô tả phương án kỹ thuật triển khai hệ thống giám sát của đơn vị vận hành hệ thống thông tin cho đơn vị chuyên trách an toàn thông tin, an ninh mạng. Mô tả đối tượng được giám sát, bao gồm các thông tin cơ bản sau đây: địa chỉ IP, tên miền, dịch vụ cung cấp, tên và phiên bản hệ điều hành, phần mềm máy chủ web; vị trí đặt hệ thống giám sát của đơn vị vận hành hệ thống thông tin, dung lượng các đường truyền kết nối vào đối tượng giám sát của đơn vị vận hành hệ thống thông tin, các thông tin dự kiến thu thập và giao thức thu thập, ví dụ cảnh báo của hệ thống phát hiện xâm nhập (Intrusion Detection System), nhật ký tường lửa (log firewall), nhật ký máy chủ web (log web server), v.v...

g) Năng lực lưu trữ thông tin giám sát tối thiểu đạt mức trung bình 30 ngày hoạt động trong điều kiện bình thường.

h) Cung cấp thông tin giám sát theo thời gian thực, định kỳ hoặc đột xuất có yêu cầu của đơn vị chuyên trách an toàn thông tin, an ninh mạng.

4. Chia sẻ thông tin giám sát.

a) Các thông tin chia sẻ, cung cấp và trao đổi bao gồm các thông tin về tấn công, rủi ro, sự cố an toàn thông tin mạng; các phương thức, thủ đoạn, nguồn gốc tấn công; các tác động, ảnh hưởng do sự cố gây ra; biện pháp quản lý, kỹ thuật để xử lý, khắc phục

b) Thông tin giám sát mã độc phải được chia sẻ với Trung tâm Giám sát an toàn không gian mạng quốc gia do Bộ Thông tin và Truyền thông quản lý theo quy định của pháp luật và hướng dẫn của Bộ Thông tin và Truyền thông.

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

1. Các đơn vị, cá nhân khi phát hiện dấu hiệu tấn công hoặc sự cố an toàn thông tin, an ninh mạng cần báo ngay cho đơn vị chuyên trách về an toàn thông tin, an ninh mạng.

2. Khi xảy ra sự cố an toàn thông tin, an ninh mạng thuộc loại hình tấn công mạng, đơn vị vận hành hệ thống thông tin thực hiện báo cáo theo quy định tại điểm a khoản 1 Điều 11 Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ và Điều 9 Thông tư số 20/2017/TT-BTTT ngày 12 tháng 9 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông và tổ chức khắc phục, xử lý kịp thời. Quy trình ứng cứu sự cố an toàn thông tin mạng theo quy định tại Điều 13, Điều 14 Quyết định 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ và Điều 11 Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông.

Điều 14. Kiểm tra, đánh giá an toàn thông tin, an ninh mạng

1. Nội dung kiểm tra, đánh giá:

a) Kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn thông tin, an ninh mạng theo cấp độ.

b) Đánh giá hiệu quả của biện pháp bảo đảm an toàn thông tin, an ninh mạng đối với hệ thống thông tin.

c) Đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống.

d) Kiểm tra, đánh giá khác do đơn vị vận hành hệ thống thông tin quy định.

2. Hình thức và thời gian kiểm tra, đánh giá:

a) Kiểm tra, đánh giá định kỳ theo kế hoạch của đơn vị vận hành hệ thống thông tin; kiểm tra thực hiện định kỳ theo phương án bảo đảm an toàn hệ thống thông tin theo cấp độ đã được phê duyệt của đơn vị chuyên trách an toàn thông tin, an ninh mạng.

b) Kiểm tra, đánh giá đột xuất theo yêu cầu của cấp có thẩm quyền.

c) Hình thức thực hiện: Tự thực hiện hoặc thuê dịch vụ.

CHƯƠNG III
TRÁCH NHIỆM CỦA CÁC ĐƠN VỊ, TỔ CHỨC, CÁ NHÂN

Điều 15. Trách nhiệm của các đơn vị, tổ chức thuộc Bộ

1. Thực hiện đúng các quy định liên quan tại Quy chế này.

2. Thủ trưởng các đơn vị, tổ chức có trách nhiệm phổ biến, quán triệt Quy chế này đến toàn thể cán bộ, công chức, viên chức, người lao động trong đơn vị, nghiêm túc tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trước Bộ trưởng trong công tác bảo đảm an toàn thông tin, an ninh mạng máy tính tại đơn vị mình.

3. Phối hợp, cung cấp thông tin và tạo điều kiện cho cán bộ kỹ thuật triển khai công tác kiểm tra, khắc phục sự cố xảy ra một cách kịp thời, nhanh chóng và đạt hiệu quả.

4. Không chuyển đổi mục đích sử dụng máy tính dùng để soạn thảo, lưu trữ thông tin mật hoặc có nội dung bí mật nhà nước sang máy tính kết nối mạng và ngược lại khi chưa có giải pháp hủy dữ liệu.

5. Đề nghị Trung tâm Tin học cấp thiết bị lưu trữ ngoài (USB) do Ban Cơ yếu Chính phủ cung cấp để sử dụng cho việc soạn thảo, lưu tài liệu mật phục vụ công việc của đơn vị. Đơn vị có trách nhiệm quản lý thiết bị lưu trữ ngoài quy định của pháp luật hiện hành về bảo vệ bí mật nhà nước.

Điều 16. Trách nhiệm của cán bộ, công chức, viên chức và người lao động.

1. Thực hiện đúng các quy định liên quan tại Quy chế này.

2. Không được tự ý gỡ bỏ các phần mềm phòng chống mã độc, các phần mềm an toàn an ninh mạng do đơn vị chuyên trách an toàn thông tin, an ninh mạng của Bộ cài đặt ra khỏi máy tính khi sử dụng mạng của Bộ.

3. Không đặt chế độ tự động đăng nhập vào các hệ thống thông tin. Có trách nhiệm bảo mật tài khoản truy cập được cấp, không giao tài khoản, mật khẩu cá nhân cho người khác. Máy tính cá nhân phải được khóa khi không sử dụng và tắt trước khi về.

4. Không sử dụng hệ thống mạng của Bộ tạo ra, cài đặt, phát tán phần mềm độc hại; bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của đơn vị, tổ chức, cá nhân trong và ngoài Bộ; xâm nhập, sửa đổi, xóa bỏ nội dung thông tin của đơn vị, tổ chức, cá nhân trong và ngoài Bộ.

5. Không cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin.

6. Không kết nối mạng đối với thiết bị chứa thông tin, dữ liệu thuộc bí mật nhà nước.

7. Không tự ý đấu nối thiết bị mạng và thiết bị cá nhân không phục vụ mục đích công vụ vào mạng của Bộ

8. Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm mã độc trên máy tính cá nhân *(ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu...)*, người sử dụng phải tắt máy và thông báo trực tiếp cho bộ phận kỹ thuật của đơn vị quản lý, vận hành hệ thống thông tin để được hỗ trợ, xử lý.

9. Thực hiện sao lưu dữ liệu trên máy tính cá nhân.

10. Khi thực hiện nhiệm vụ đảm bảo an toàn thông tin, an ninh mạng, quản trị, vận hành hệ thống phải có trách nhiệm giữ bí mật thông tin về hệ thống thông tin được giao quản lý, vận hành.

Điều 17. Trách nhiệm của các đơn vị quản lý, vận hành hệ thống thông tin

1. Thực hiện đúng các quy định liên quan tại các Điều 5, 6, 7, 8, 9, 10, 11, 12, 13, 14 Quy chế này.

2. Tổ chức thực hiện bảo đảm an toàn thông tin, an ninh mạng theo cấp độ đối với hệ thống thông tin do đơn vị quản lý, vận hành. Bố trí nhân sự được đào tạo, bồi dưỡng về an toàn thông tin và có cam kết giữ bí mật khi thực hiện nhiệm vụ bảo đảm an toàn thông tin, an ninh mạng.

3. Tổ chức triển khai phần mềm phòng chống mã độc cho máy tính cá nhân và máy chủ thuộc hệ thống mạng do đơn vị quản lý, vận hành, phối hợp với đơn vị chuyên trách về an toàn thông tin, an ninh mạng triển khai các hoạt động chia sẻ thông tin, dữ liệu, giám sát an toàn thông tin, điều phối, ứng cứu sự cố an toàn thông tin mạng.

4. Tổ chức triển khai, duy trì, bảo đảm kết nối đường truyền giữa hệ thống mạng do đơn vị quản lý vận hành với Trung tâm dữ liệu của Bộ để thực hiện chia sẻ, tích hợp dữ liệu.

5. Cung cấp thông tin về an toàn thông tin, an ninh mạng theo yêu cầu của đơn vị chuyên trách về an toàn thông tin, an ninh mạng để tổng hợp, xây dựng báo cáo an toàn thông tin, an ninh mạng của Bộ.

6. Tổ chức xây dựng, cập nhật các quy định quản lý về chính sách, kỹ thuật và quy trình quản trị, vận hành, cập nhật.

7. Xây dựng và triển khai kế hoạch ứng phó sự cố an toàn thông tin, an ninh mạng, tổ chức diễn tập ứng cứu sự cố an toàn thông tin, an ninh mạng thông tin mạng đối với các hệ thống thông tin do đơn vị quản lý, tổ chức tối thiểu 01 lần/năm; tham gia diễn tập ứng cứu sự cố do đơn vị chuyên trách về an toàn thông tin, an ninh mạng tổ chức.

8. Triển khai biện pháp quản lý, kỹ thuật để phòng ngừa, phát hiện, ngăn chặn, gỡ bỏ thông tin có nội dung quy định tại các khoản 1, 2, 3, 4 và 5 Điều 16, điểm a, b, c, d và e khoản 1 Điều 19 Luật An ninh mạng năm 2018 trên hệ thống thông tin thuộc phạm vi quản lý khi có yêu cầu của đơn vị chuyên trách an toàn thông tin, an ninh mạng của Bộ, lực lượng chuyên trách bảo vệ an ninh mạng; Triển khai biện pháp quản lý, kỹ thuật để phòng ngừa, phát hiện, ngăn chặn hành vi gián điệp mạng, xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên hệ thống thông tin và kịp thời gỡ bỏ thông tin liên quan đến hành vi này.

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

10. Phối hợp, thực hiện yêu cầu của đơn vị chuyên trách về an toàn thông tin, an ninh mạng, lực lượng chuyên trách an ninh mạng về phòng, chống gián điệp mạng, bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên hệ thống thông tin. Phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an trong phòng ngừa, phát hiện, xử lý tình huống nguy hiểm về an ninh mạng.

11. Thường xuyên rà soát, kiểm tra hệ thống thông tin thuộc phạm vi quản lý nhằm loại trừ nguy cơ khủng bố mạng.

Điều 18. Trách nhiệm của Trung tâm Tin học

1. Thực hiện đúng các quy định liên quan tại các Điều 5, 6, 7, 8, 9, 10, 11, 12, 13, 14 Quy chế này.

2. Tham mưu cho Bộ trưởng về công tác bảo đảm an toàn thông tin, an ninh mạng.

3. Thực hiện trách nhiệm của đơn vị chuyên trách về an toàn thông tin, an ninh mạng và lực lượng bảo vệ an ninh mạng của Bộ.

4. Tổ chức xây dựng, quản lý vận hành trung tâm giám sát an toàn, an ninh mạng của Bộ. Chia sẻ thông tin giám sát an toàn thông tin mạng với Trung tâm Giám sát an toàn không gian mạng quốc gia do Bộ Thông tin và Truyền thông

quản lý theo quy định của pháp luật và hướng dẫn của Bộ Thông tin và Truyền thông.

5. Lập kế hoạch, thực hiện kiểm tra, đánh giá an toàn thông tin, an ninh mạng. Chủ trì kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ đối với các đơn vị quản lý, vận hành hệ thống thông tin.

6. Chủ trì phối hợp với các cơ quan quản lý nhà nước trong việc xử lý, ứng cứu sự cố an toàn thông tin, an ninh mạng. Thực hiện nghĩa vụ thành viên của Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia.

7. Cấp, hủy tài khoản, quyền truy cập các hệ thống thông tin đối với các cá nhân, đơn vị.

8. Tổ chức thực hiện cấp thiết bị lưu trữ ngoài (USB) do Ban Cơ yếu Chính phủ cung cấp cho các đơn vị thuộc Bộ để sử dụng cho việc soạn thảo, lưu tài liệu mật.

9. Tổ chức thực hiện tuyên truyền, phổ biến, tập huấn, nâng cao nhận thức, kỹ năng về an toàn thông tin, an ninh mạng cho cán bộ, công chức, viên chức và người lao động của Bộ.

10. Hằng năm, tổ chức diễn tập ứng cứu sự cố an toàn thông tin, an ninh mạng.

11. Tổ chức thu thập, phát hiện các thông tin liên quan tới lĩnh vực quản lý nhà nước của Bộ Kế hoạch và Đầu tư trên không gian mạng.

12. Thực hiện báo cáo cấp có thẩm quyền khi phát hiện hành vi vi phạm pháp luật về an toàn thông tin, an ninh mạng.

13. Thực hiện thông báo cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an khi phát hiện hành vi vi phạm pháp luật về an ninh mạng sau khi báo cáo và được sự đồng ý của cấp có thẩm quyền.

Điều 19. Trách nhiệm của Văn phòng Bộ

1. Phối hợp với Trung tâm Tin học đảm bảo an toàn thông tin, an ninh Trung tâm điều hành.

2. Đảm bảo việc mua sắm tập trung máy tính kèm theo bản quyền phần mềm hệ điều hành, bộ phần mềm văn phòng.

3. Đảm bảo bố trí máy tính, máy in riêng không kết nối mạng cho các đơn vị để soạn thảo tài liệu mật.

CHƯƠNG IV
TỔ CHỨC THỰC HIỆN

Điều 20. Khen thưởng và xử lý vi phạm

1. Hằng năm, Trung tâm Tin học dựa trên các kết quả kiểm tra, giám sát và báo cáo để xác lập bảng xếp hạng an toàn thông tin, an ninh mạng máy tính của các đơn vị thuộc Bộ, báo cáo lãnh đạo Bộ, đồng thời gửi đơn vị thực hiện nhiệm vụ thi đua khen thưởng làm cơ sở đề xuất Bộ trưởng khen thưởng theo quy định hiện hành.

2. Các đơn vị, tổ chức, cá nhân có hành vi vi phạm Quy chế này tùy theo tính chất, mức độ vi phạm mà bị nhắc nhở, xử lý theo quy định của pháp luật hiện hành.

Điều 21. Điều khoản thi hành

1. Trung tâm Tin học chủ trì, phối hợp với các cơ quan, tổ chức, đơn vị có liên quan tổ chức hướng dẫn, theo dõi và đôn đốc việc thực hiện các quy định của Quy chế này.

2. Trong quá trình thực hiện Quy chế này, nếu có những vấn đề khó khăn, vướng mắc, các đơn vị phản ảnh về Trung tâm Tin học để tổng hợp, trình Bộ trưởng xem xét, quyết định cho phù hợp với điều kiện thực tế và quy định của pháp luật hiện hành./.