

BỘ Y TẾ

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập - Tự do - Hạnh phúc

Số: /QĐ-BYT

Hà Nội, ngày tháng năm 2024

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an toàn thông tin, an ninh mạng của Bộ Y tế

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 95/2022/NĐ-CP ngày 15 tháng 11 năm 2022 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Y tế;

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 04/2019/NĐ-CP ngày 27 tháng 12 năm 2019 của Chính phủ quy định chi tiết trình tự, thủ tục áp dụng một số biện pháp bảo vệ an ninh mạng;

Căn cứ Nghị định số 53/2022/NĐ-CP ngày 15 tháng 8 năm 2022 của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng;

Căn cứ Nghị định số 13/2023/NĐ-CP ngày 17 tháng 4 năm 2023 của Chính phủ về bảo vệ dữ liệu cá nhân;

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 Quyết định số 12/QĐ-TTg ngày 01 tháng 02 năm 2019 của Thủ tướng Chính phủ ban hành Kế hoạch triển khai thi hành Luật An ninh mạng;

Căn cứ Chỉ thị số 01/CT-TTg ngày 18 tháng 02 năm 2021 của Thủ tướng Chính phủ về tăng cường công tác bảo vệ an ninh mạng trong tình hình hiện nay;

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của 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 27/2017/TT-BTTTT ngày 20 tháng 10 năm 2017 của Bộ Thông tin và Truyền thông quy định về quản lý, vận hành, kết nối, sử dụng và bảo đảm an toàn thông tin trên mạng truyền số liệu chuyên dùng của các cơ

quan Đảng, Nhà nước; Thông tư số 12/2019/TT-BTTTT ngày 05 tháng 11 năm 2019 của Bộ Thông tin và Truyền thông về Sửa đổi, bổ sung một số điều của Thông tư số 27/2017/TT-BTTTT ngày 20 tháng 10 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về quản lý, vận hành, kết nối, sử dụng và bảo đảm an toàn thông tin trên mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước;

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

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của 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;

Theo đề nghị của Cục trưởng Cục Khoa học công nghệ và Đào tạo;

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này “Quy chế bảo đảm an toàn thông tin, an ninh mạng của Bộ Y tế”.

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày ký, ban hành và thay thế Quyết định số 4159/QĐ-BYT ngày 13 tháng 10 năm 2014 của Bộ trưởng Bộ Y tế ban hành quy định về bảo đảm an toàn thông tin y tế điện tử tại các đơn vị trong ngành y tế.

Điều 3. Các Ông / Bà: Chánh Văn phòng Bộ, Cục trưởng Cục Khoa học công nghệ và Đào tạo, Giám đốc Trung tâm Thông tin y tế Quốc gia, Thủ trưởng các đơn vị thuộc và trực thuộc Bộ; các cơ quan, đơn vị, tổ chức và cá nhân liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:

- Như Điều 3;
- Bộ trưởng (để báo cáo);
- Các Thứ trưởng (để phối hợp);
- Các Bộ: Công an, TTTT;
- Lưu: VT, K2ĐT.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Trần Văn Thuấn

BỘ Y TẾ**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 của Bộ Y tế
(Kèm theo Quyết định số /QĐ-BYT ngày / /2024 của Bộ trưởng Bộ Y tế)

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 các hoạt động ứng dụng công nghệ thông tin của Bộ Y tế (sau đây gọi tắt là Bộ).

2. Đối tượng áp dụng:

a) Các cơ quan, đơn vị thuộc và trực thuộc Bộ (sau đây gọi tắt là đơn vị) và cán bộ, công chức, viên chức, người lao động của các đơn vị thuộc và trực thuộc Bộ (sau đây gọi tắt là cá nhân) tham gia hoạt động ứng dụng công nghệ thông tin của Bộ.

b) Cơ quan, tổ chức, cá nhân có kết nối vào hệ thống mạng của Bộ.

c) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ công nghệ thông tin và an toàn thông tin mạng cho các đơn vị thuộc, trực thuộc Bộ.

Điều 2. Giải thích từ ngữ

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

1. *Trung tâm dữ liệu (Data center)*: là tòa nhà hoặc một phần của tòa nhà có chức năng chính là chứa một phòng máy chủ và các khu vực hỗ trợ.

2. *Phòng máy chủ*: bao gồm hệ thống máy chủ, thiết bị chuyển mạch, thiết bị định tuyến, thiết bị lưu trữ, thiết bị bảo đảm an toàn thông tin mạng, thiết bị ngoại vi, thiết bị phụ trợ, đường truyền kết nối Internet và thiết bị phòng cháy, chữa cháy, chống sét và các thiết bị khác theo quy định.

3. *Trang thiết bị công nghệ thông tin cá nhân*: bao gồm máy tính để bàn, máy tính xách tay, thiết bị số (máy tính bảng, điện thoại thông minh,...) cá nhân.

Điều 3. Phạm vi bảo đảm an toàn thông tin, an ninh mạng

1. Trung tâm dữ liệu/Phòng máy chủ của Bộ và các đơn vị thuộc, trực thuộc Bộ.

2. Hệ thống mạng nội bộ (LAN), mạng diện rộng (WAN), mạng có kết nối Internet.

3. Máy tính, thiết bị ngoại vi, hệ thống thông tin, phần mềm, ứng dụng nghiệp vụ và cơ sở dữ liệu phục vụ công tác quản lý, điều hành, nghiệp vụ của Bộ và các đơn vị thuộc, trực thuộc Bộ.

4. Các hệ thống thông tin và cơ sở dữ liệu phục vụ công tác quản lý, điều hành, nghiệp vụ của Bộ.

5. Các trang thiết bị công nghệ thông tin cá nhân.

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

1. Bảo đảm an toàn thông tin, an ninh mạng là yêu cầu bắt buộc, thường xuyên, liên tục, đồng bộ từ khi thiết kế, xây dựng, vận hành, nâng cấp và hủy bỏ (dừng hoạt động) hệ thống thông tin. Bảo đảm an toàn thông tin, an ninh mạng phải tuân thủ các nguyên tắc chung, được quy định tại Điều 4 Luật An toàn thông tin mạng, Điều 4 Luật An ninh mạng, 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 (Nghị định số 85/2016/NĐ-CP).

2. Đơn vị vận hành hệ thống thông tin có trách nhiệm bảo đảm an toàn thông tin, an ninh mạng đối với hệ thống thông tin của đơn vị mình quản lý và sử dụng; bố trí nhân sự để sẵn sàng xử lý sự cố an toàn thông tin, an ninh mạng đối với các hệ thống thông tin do đơn vị mình quản lý.

3. Cá nhân có trách nhiệm bảo đảm an toàn thông tin, an ninh mạng trong phạm vi xử lý công việc của mình theo quy định của Nhà nước và của Bộ.

4. Thông tin mật, thông tin thuộc Danh mục bí mật nhà nước ngành y tế phải được bảo vệ theo quy định của Nhà nước, quy định của Bộ Y tế về công tác bảo vệ bí mật nhà nước và các nội dung tương ứng trong Quy chế này.

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

Điều 5. Các hành vi bị nghiêm cấm

1. Các hành vi bị nghiêm cấm được quy định tại Điều 7 Luật An toàn thông tin mạng và Điều 8 Luật An ninh mạng.

2. Tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập mạng không dây của cá nhân vào mạng nội bộ; trên cùng một thiết bị thực hiện đồng thời truy cập vào mạng nội bộ và truy cập Internet bằng thiết bị kết nối Internet của cá nhân (như điện thoại di động, máy tính bảng, máy tính xách tay, USB 3G/4G/5G, ...).

3. Tự ý thay đổi, gỡ bỏ các biện pháp an toàn thông tin, an ninh mạng được cài đặt trên thiết bị công nghệ thông tin phục vụ công việc; tự ý thay thế, lắp mới, tháo đổi thành phần của máy tính phục vụ công việc.

4. Tạo ra, cài đặt, phát tán phần mềm độc hại.

5. Cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin; ngăn chặn việc truy nhập đến thông tin của cơ quan, cá nhân khác trên môi trường mạng, trừ trường hợp pháp luật cho phép.

6. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của cơ quan, cá nhân khác trên môi trường mạng.

7. Các hành vi khác làm mất an toàn, bí mật thông tin của cơ quan, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

Chương II

QUY ĐỊNH BẢO ĐẢM AN TOÀN THÔNG TIN, AN NINH MẠNG

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

1. Trung tâm Thông tin y tế Quốc gia là đơn vị quản lý, vận hành Trung tâm dữ liệu của Bộ, có trách nhiệm xây dựng nội quy, quy chế quản lý, vận hành, bảo đảm an toàn thông tin, an ninh mạng đối với Trung tâm dữ liệu của Bộ.

2. Đơn vị quản lý vận hành Trung tâm dữ liệu/Phòng máy chủ của các đơn vị có trách nhiệm xây dựng nội quy, quy chế quản lý, vận hành, bảo đảm an toàn thông tin, an ninh mạng đối với Trung tâm dữ liệu/Phòng máy chủ của đơn vị.

3. Bảo đảm vận hành Trung tâm dữ liệu/Phòng máy chủ

a) Trung tâm dữ liệu/Phòng máy chủ là khu vực hạn chế tiếp cận, chỉ những cá nhân có quyền, nhiệm vụ theo quy định của thủ trưởng đơn vị mới được phép vào Trung tâm dữ liệu/Phòng máy chủ. Việc vào, ra Trung tâm dữ liệu/Phòng máy chủ phải được kiểm soát bằng thiết bị bảo vệ (quẹt thẻ, vân tay, sinh trắc học,...);

b) Các thiết bị kết nối mạng, thiết bị bảo mật quan trọng như tường lửa (firewall), thiết bị định tuyến (router), hệ thống máy chủ, hệ thống lưu trữ SAN, NAS, ... phải được đặt trong Trung tâm dữ liệu/Phòng máy chủ và phải được thiết lập cơ chế bảo vệ, theo dõi phát hiện xâm nhập, biện pháp kiểm soát truy nhập, 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. Đơn vị chủ quản Trung tâm dữ liệu/Phòng máy chủ có trách nhiệm xây dựng nội quy hoặc hướng dẫn làm việc khu vực này.

c) Trung tâm dữ liệu/Phòng máy chủ phải được trang bị hệ thống lưu điện đủ công suất và duy trì thời gian hoạt động của các máy chủ ít nhất 15 phút khi có sự cố mất điện.

Điều 7. Bảo đảm an toàn thông tin, an ninh của hệ thống mạng

1. Hệ thống mạng nội bộ (LAN) phải được thiết kế số lượng phân vùng mạng theo cấp độ hệ thống thông tin. Dữ liệu trao đổi giữa các vùng mạng phải được quản lý giám sát bởi các hệ thống các thiết bị mạng, thiết bị bảo mật. Căn cứ điều kiện, yêu cầu thực tế về bảo mật dữ liệu, đơn vị là chủ quản hệ thống mạng nội bộ chủ động triển khai xây dựng mô hình, giải pháp an toàn, bảo mật bao gồm:

a) Kiểm soát truy nhập từ bên ngoài mạng (sử dụng các giao thức mạng có hỗ trợ chức năng mã hóa thông tin như SSH, SSL/TLS, VPN hoặc tương đương).

b) Kiểm soát truy nhập từ bên trong mạng (quản lý các thiết bị đầu cuối, máy tính người sử dụng kết nối vào hệ thống mạng; giám sát, phát hiện và ngăn chặn truy nhập từ bên trong mạng đến các địa chỉ Internet bị cấm truy nhập).

c) Phòng, chống xâm nhập và phần mềm độc hại, bảo vệ các vùng mạng máy chủ công cộng, máy chủ nội bộ, máy chủ cơ sở dữ liệu và vùng mạng nội bộ. Phát hiện và vô hiệu hóa tất cả các dịch vụ không cần thiết tại từng vùng mạng có thể gây mất an toàn, an ninh thông tin.

d) Cấu hình chức năng xác thực trên các thiết bị kết nối mạng để xác thực người sử dụng quản trị thiết bị trực tiếp hoặc từ xa.

đ) Đối với mạng không dây, phải có giải pháp bảo toàn tính toàn vẹn và bí mật của thông tin được truyền đưa trên môi trường mạng, có hướng dẫn bảo đảm an toàn thông tin dành cho các thiết bị đầu cuối khi kết nối vào mạng. Việc thay đổi mật khẩu định kỳ, các điểm truy nhập không dây phải được bảo vệ, tránh bị tiếp cận trái phép.

e) Hệ thống máy chủ phải có chức năng tự động cập nhật bản ghi và lưu nhật ký hệ thống trong khoảng thời gian nhất định (tối thiểu 06 tháng), lưu trữ thông tin kết nối mạng, quá trình đăng nhập vào máy chủ, các thao tác cấu hình hệ thống, lỗi phát sinh trong quá trình hoạt động và các thông tin liên quan về an toàn thông tin để bảo đảm công tác khắc phục sự cố, điều tra về an toàn thông tin. Xóa sạch thông tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng.

2. Áp dụng các biện pháp kỹ thuật cần thiết bảo đảm an toàn thông tin, an ninh mạng trong hoạt động kết nối Internet, tối thiểu đáp ứng các yêu cầu sau:

a) Có hệ thống tường lửa, hệ thống bảo vệ kiểm soát truy nhập Internet, đáp ứng nhu cầu kết nối đồng thời; hỗ trợ các công nghệ mạng riêng ảo; quản lý luồng dữ liệu ra, vào và có khả năng bảo vệ hệ thống trước các loại tấn công mạng.

b) Lọc bỏ, không cho phép truy nhập các trang tin có nghi ngờ chứa mã độc hoặc các nội dung không phù hợp.

c) Chỉ thiết lập kết nối Internet cho các máy chủ và thiết bị công nghệ thông tin cần phải có giao tiếp với Internet.

3. Các đường truyền dữ liệu, đường truyền Internet và các hệ thống dây dẫn mạng LAN, WAN phải được lắp đặt trong ống, máng che đậy kín, hạn chế khả năng tiếp cận trái phép. Ngắt kết nối cổng Ethernet không sử dụng, đặc biệt là ở khu vực làm việc chung của các cơ quan, đơn vị.

Điều 8. Bảo đảm an toàn thông tin, an ninh mạng đối với các hệ thống thông tin quản lý và các cơ sở dữ liệu của Bộ

1. Bảo đảm an toàn thông tin, an ninh mạng trong xây dựng, nâng cấp hệ thống thông tin và các cơ sở dữ liệu.

a) Khi xây dựng mới hoặc nâng cấp hệ thống thông tin, các cơ sở dữ liệu, đơn vị vận hành hệ thống thông tin có trách nhiệm xây dựng phương án bảo đảm an toàn, an ninh cho các hệ thống thông tin, cơ sở dữ liệu; rà soát cấp độ an toàn của hệ thống thông tin và thực hiện điều chỉnh hồ sơ đề xuất cấp độ trong trường hợp cần thiết.

b) Quá trình tổ chức xây dựng, nâng cấp hệ thống thông tin phải tuân thủ phương án bảo đảm an toàn thông tin, an ninh mạng và các quy định liên quan.

2. Bảo đảm an toàn thông tin, an ninh mạng khi đưa vào khai thác sử dụng hệ thống thông tin và các cơ sở dữ liệu.

a) Bảo đảm an toàn thông tin, an ninh mạng trong quản lý hệ thống thông tin:

- Chủ quản hệ thống thông tin chịu trách nhiệm bảo đảm an toàn thông tin cho các hệ thống thông tin theo quy định tại các Điều 22, 23, 24 Luật An toàn thông tin mạng và Khoản 2 Điều 17, các Điều 18, 19, 20, 21, 22 của Luật An ninh mạng.

b) Bảo đảm an toàn thông tin, an ninh mạng trong vận hành hệ thống thông tin:

- Đơn vị vận hành hệ thống thông tin phải thực hiện các quy định về bảo đảm an toàn thông tin theo Điều 22 Nghị định số 85/2016/NĐ-CP.

- Đơn vị vận hành hệ thống thông tin 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; lưu trữ đầy đủ nhật ký hệ thống thông tin để phục vụ quản lý và kiểm soát thông tin.

c) Bảo đảm an toàn thông tin, an ninh mạng trong quản lý và sử dụng tài khoản truy cập các hệ thống thông tin:

- Khi được cấp tài khoản sử dụng hệ thống thông tin, cá nhân phải đổi mật khẩu trong lần đăng nhập đầu tiên; mật khẩu phải đủ mạnh (có độ dài ít nhất 8 ký tự, gồm: chữ cái hoa và thường, chữ số và ký tự đặc biệt); thay đổi mật khẩu tối thiểu 06 tháng/lần. Cá nhân có trách nhiệm bảo mật thông tin tài khoản truy nhập, không chia sẻ mật khẩu với người khác. Đăng xuất hệ thống thông tin khi không sử dụng.

- Khi cá nhân thay đổi vị trí, chuyển công tác, thôi việc, nghỉ hưu hoặc cần tạm khóa quyền truy cập tài khoản người sử dụng, đơn vị quản lý cá nhân đó phải thông báo cho đơn vị vận hành hệ thống thông tin thực hiện điều chỉnh, tạm khóa, thu hồi hoặc hủy bỏ tài khoản.

- Đơn vị vận hành hệ thống thông tin có quyền khóa quyền truy cập của tài khoản trong trường hợp tài khoản đó thực hiện các hành vi tấn công hoặc để xảy ra vấn đề mất an toàn thông tin. Hạn chế dùng chung tài khoản quản trị.

d) Bảo đảm an toàn thông tin mức ứng dụng

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

- 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 khuyến khích việc đăng nhập tự động.

- Thiết lập, phân quyền truy nhập, 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.

- Chỉ cho phép sử dụng các giao thức mạng có hỗ trợ chức năng mã hóa thông tin như SSH, SSL, VPN hoặc tương đương khi truy nhập, 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 chuyên trách công nghệ thông tin quản lý.

- Ghi và lưu giữ bản ghi nhật ký hệ thống của phần mềm, ứng dụng trong khoảng thời gian tối thiểu 03 tháng với những thông tin cơ bản: thời gian, địa chỉ, tài khoản (nếu có), nội dung truy nhập và sử dụng phần mềm, ứng dụng; các lỗi phát sinh trong quá trình hoạt động; thông tin đăng nhập khi quản trị.

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

- Phần mềm, ứng dụng cần được kiểm tra phát hiện và khắc phục các điểm yếu về an toàn, an ninh thông tin trước khi đưa và thiết bị kết nối mạng đang hoạt động thuộc hệ thống mạng nội bộ.

đ) Bảo đảm an toàn thông tin mức dữ liệu, cơ sở dữ liệu

- Đơn vị phải thực hiện bảo vệ thông tin, dữ liệu liên quan đến hoạt động công vụ, thông tin có nội dung quan trọng, nhạy cảm hoặc không phải là thông tin công khai bằng các biện pháp như: 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.

- Đơn vị cần triển khai hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng; phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau; thực hiện sao lưu dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

- Đơn vị cần bố trí máy tính riêng không kết nối mạng, đặt mặt khẩu, mã hóa dữ liệu và các biện pháp bảo mật khác bảo đảm an toàn thông tin để soạn thảo, lưu trữ dữ liệu, thông tin và tài liệu quan trọng ở các mức độ mật, tuyệt mật, tối mật.

- Các đơn vị thuộc, trực thuộc Bộ phải thường xuyên kiểm tra, giám sát các hoạt động chia sẻ, gửi, nhận thông tin, dữ liệu trong hoạt động nội bộ của mình; khuyến cáo việc chia sẻ, gửi, nhận thông tin trên môi trường mạng cần phải sử dụng mặt khẩu để bảo vệ thông tin.

- Đối với hoạt động trao đổi thông tin, dữ liệu với bên ngoài, đơn vị và cá nhân thực hiện trao đổi thông tin, dữ liệu ra bên ngoài cam kết và có biện pháp bảo mật thông tin, dữ liệu được trao đổi. Giao dịch trực tuyến phải được truyền đầy đủ, đúng địa chỉ, tránh bị sửa đổi, tiết lộ hoặc nhân bản một cách trái phép;

sử dụng các cơ chế xác thực mạnh, chữ ký số khi tham gia giao dịch, sử dụng các giao thức truyền thông an toàn.

Điều 9. Bảo đảm an toàn thông tin, an ninh mạng khi sử dụng máy tính và thiết bị ngoại vi

1. Máy tính và thiết bị ngoại vi của đơn vị phải được cài đặt hệ điều hành, phần mềm soạn thảo văn bản, phần mềm chuyên dụng để xử lý công việc và tuân thủ các quy định sau:

a) Chỉ cài đặt phần mềm hợp lệ (phần mềm có bản quyền thương mại, phần mềm nội bộ hoặc phần mềm mã nguồn mở được đầu tư (hoặc thuê dịch vụ) có nguồn gốc rõ ràng) và thuộc danh mục phần mềm được phép sử dụng do đơn vị có thẩm quyền của Bộ Y tế ban hành (nếu có); không được tự ý cài đặt hoặc gỡ bỏ các phần mềm khi chưa có sự đồng ý của bộ phận chuyên trách về công nghệ thông tin; thường xuyên cập nhật phần mềm và hệ điều hành.

b) Cài đặt phần mềm xử lý phần mềm độc hại và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm; thực hiện kiểm tra, rà quét phần mềm độc hại khi sao chép, mở các tập tin hoặc trước khi kết nối các thiết bị lưu trữ dữ liệu di động với máy tính của mình.

c) Khi phát hiện bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy tính (máy chạy chậm bất thường, cảnh báo từ phần mềm phòng, chống phần mềm độc hại, mất dữ liệu,...), phải tắt máy và báo trực tiếp cho bộ phận chuyên trách về công nghệ thông tin để được xử lý kịp thời.

d) Chỉ truy nhập vào các trang/công thông tin điện tử, ứng dụng trực tuyến tin cậy và các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình; sử dụng những trình duyệt an toàn; không truy nhập, mở các trang tin, thư điện tử không rõ nguồn gốc; không sử dụng tính năng lưu mật khẩu tự động hoặc đăng nhập tự động.

đ) Có trách nhiệm bảo mật tài khoản truy nhập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác. Đặt mật khẩu với độ an toàn cao (tối thiểu 8 ký tự bao gồm: có chữ thường, có chữ in hoa, có số và ký tự đặc biệt như @, #, !,...) và thay đổi mật khẩu tối thiểu 6 tháng/lần; các tài khoản đăng nhập các hệ thống phải được đăng xuất khi không sử dụng; thường xuyên xóa bộ nhớ cache và cookie trong trình duyệt trên máy tính.

e) Thực hiện thao tác khóa máy tính (sử dụng tính năng có sẵn trên máy tính) khi rời khỏi nơi đặt máy tính; tắt máy tính khi rời khỏi đơn vị.

2. Trước khi mang máy tính, thiết bị công nghệ thông tin có kết nối mạng thuộc sở hữu riêng đến nơi làm việc và kết nối với mạng nội bộ để thực hiện xử lý công việc phải báo cáo và phải được lãnh đạo đơn vị đồng ý, cho phép. Trong

trường hợp này, cá nhân phải tuân thủ đầy đủ các quy định tại các điểm a, b, c, d, đ, e khoản 1 Điều này và chịu sự giám sát của bộ phận chuyên trách về công nghệ thông tin của đơn vị.

3. Đối với văn bản có nội dung bí mật nhà nước:

a) Các đơn vị phải bố trí ít nhất một máy tính, máy in (hoặc máy phôtô) không kết nối mạng Internet, mạng máy tính, mạng viễn thông để soạn thảo các văn bản có nội dung bí mật nhà nước.

b) Công chức, viên chức, nhân viên được giao nhiệm vụ trong quá trình xử lý công việc, soạn thảo văn bản có nội dung bí mật nhà nước chỉ sử dụng máy vi tính không kết nối mạng Internet, mạng máy tính, mạng viễn thông; việc lưu trữ văn bản phải được thực hiện ở các thiết bị riêng biệt (như USB, ổ cứng di động đã được kiểm định hoặc vật có tính năng tương tự). Trường hợp không có thiết bị lưu trữ, khi soạn thảo tài liệu có nội dung bí mật phải đặt mã khóa bảo vệ bản mềm tại máy tính soạn thảo để bảo vệ bí mật nhà nước theo đúng quy định.

Điều 10. Quản lý trang thiết bị công nghệ thông tin, an toàn, an ninh thông tin đối với cá nhân

1. Quản lý trang thiết bị công nghệ thông tin đối với cá nhân:

a) Giao, gán trách nhiệm cho cá nhân hoặc tập thể quản lý, sử dụng trang thiết bị công nghệ thông tin.

b) Quy định việc sử dụng, giữ gìn bảo vệ trang thiết bị công nghệ thông tin trong các trường hợp như: mang ra khỏi cơ quan, trang thiết bị công nghệ thông tin liên quan đến dữ liệu nhạy cảm, cài đặt và cấu hình.

c) Trang thiết bị công nghệ thông tin có lưu trữ dữ liệu nhạy cảm khi thay đổi mục đích sử dụng hoặc thanh lý, đơn vị phải thực hiện các biện pháp xóa, tiêu hủy dữ liệu đó đảm bảo không có khả năng phục hồi. Trường hợp không thể tiêu hủy được dữ liệu, đơn vị phải thực hiện tiêu hủy cấu phần lưu trữ dữ liệu trên trang thiết bị công nghệ thông tin đó.

d) Thiết bị tính toán có bộ phận lưu trữ hoặc thiết bị lưu trữ khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài hoặc ngừng sử dụng phải tháo bộ phận lưu trữ khỏi thiết bị hoặc xóa thông tin, dữ liệu lưu trữ trên thiết bị (trừ trường hợp để khôi phục dữ liệu).

đ) Các đơn vị trực thuộc Bộ có trách nhiệm bảo dưỡng, bảo trì và hướng dẫn cách sử dụng, quản lý, vận hành hệ thống hạ tầng kỹ thuật của mình; chỉ định bộ phận chuyên trách về công nghệ thông tin thực hiện quản lý, vận hành và định kỳ kiểm tra, sửa chữa, bảo trì thiết bị (bao gồm thiết bị đang hoạt động và thiết bị dự phòng).

2. Quản lý an toàn, an ninh thông tin đối với cá nhân:

a) Các đơn vị thuộc, trực thuộc Bộ phải xây dựng các yêu cầu, trách nhiệm bảo đảm an toàn, an ninh thông tin đối với từng vị trí công việc. Sau khi tuyển dụng, tiếp nhận nhân sự mới, đơn vị phải có trách nhiệm phổ biến cho nhân sự mới các quy định về bảo đảm an toàn, an ninh thông tin tại đơn vị; đối với các vị trí tiếp xúc, quản lý các thông tin, dữ liệu quan trọng hoặc quản trị các hệ thống thông tin quan trọng, đơn vị phải yêu cầu nhân sự mới cam kết bảo mật thông tin bằng văn bản hoặc cam kết trong hợp đồng làm việc, hợp đồng lao động.

b) Các đơn vị thuộc, trực thuộc Bộ phải thường xuyên tổ chức quán triệt các quy định về an toàn, an ninh thông tin, nhằm nâng cao nhận thức về trách nhiệm bảo đảm an toàn thông tin của từng cá nhân trong đơn vị.

c) Các đơn vị thuộc, trực thuộc Bộ phải xây dựng quy trình cấp mới, quản lý và thu hồi tài khoản, phân quyền truy cập các hệ thống thông tin và tất cả các tài sản liên quan đến hệ thống thông tin đối với các cá nhân do đơn vị quản lý.

d) Khi cá nhân chấm dứt hoặc thay đổi công việc, cơ quan, đơn vị phải:

- Xác định rõ trách nhiệm của cán bộ, nhân viên và các bên liên quan trong quản lý, sử dụng các tài sản công nghệ thông tin được giao.
- Lập biên bản bàn giao tài sản công nghệ thông tin.
- Thay đổi hoặc thu hồi quyền truy cập các hệ thống thông tin.

Điều 11. Xác định cấp độ và phương án bảo đảm an toàn thông tin, an ninh mạng hệ thống thông tin

1. Các hệ thống thông tin phải thực hiện bảo đảm an toàn thông tin, an ninh mạng theo cấp độ theo quy định tại Nghị định số 85/2016/NĐ-CP và Nghị định số 53/2022/NĐ-CP

2. Chủ quản hệ thống thông tin

a) Bộ Y tế là chủ quản hệ thống thông tin đối với các hệ thống do Bộ quyết định đầu tư hoặc Bộ được giao làm chủ đầu tư nhiệm vụ, dự án xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin. Bộ Y tế ủy quyền cho các đơn vị thuộc, trực thuộc Bộ quản lý trực tiếp các hệ thống do Bộ làm chủ quản thông qua một trong các văn bản sau: Quyết định phê duyệt dự án, trong đó giao đơn vị làm chủ đầu tư dự án; Thông tư của Bộ Y tế hoặc Quyết định của Bộ trưởng Bộ Y tế có nội dung giao đơn vị làm nhiệm vụ quản lý hệ thống; Văn bản ủy quyền theo quy định tại khoản 3 Điều 4 Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của 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 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ (Thông tư số

12/2022/TT-BTTTT).

b) Các đơn vị thuộc, trực thuộc Bộ là chủ quản hệ thống thông tin do đơn vị quyết định đầu tư dự án xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin; là chủ quản hệ thống thông tin do đơn vị phê duyệt đề cương, dự toán chi tiết; quản lý trực tiếp các hệ thống do Bộ Y tế ủy quyền theo quy định tại điểm a khoản này.

c) Chủ quản hệ thống thông tin (hoặc đơn vị được ủy quyền quản lý trực tiếp hệ thống thông tin) thực hiện trách nhiệm theo quy định tại Điều 20 Nghị định 85/2016/NĐ-CP.

3. Đơn vị vận hành hệ thống thông tin

a) Các hệ thống thông tin trước khi đưa vào khai thác, sử dụng phải được giao cho đơn vị quản lý, vận hành.

b) Đơn vị vận hành hệ thống thông tin theo quy định tại Điều 5 Thông tư số 12/2022/TT-BTTTT.

4. Đơn vị chuyên trách về an toàn thông tin

a) Cục Khoa học công nghệ và Đào tạo là đơn vị chuyên trách về an toàn thông tin của Bộ Y tế.

b) Đơn vị (hoặc bộ phận) chuyên trách về công nghệ thông tin đồng thời là đơn vị chuyên trách về an toàn thông tin tại các đơn vị thuộc, trực thuộc Bộ.

5. Thẩm quyền xác định cấp độ an toàn hệ thống thông tin

a) Đơn vị lập hồ sơ đề xuất cấp độ: Đối với các hệ thống thông tin thuộc các nhiệm vụ, dự án đang trong giai đoạn lập dự án, đơn vị lập dự án lập hồ sơ đề xuất cấp độ; Đối với các hệ thống thông tin thuê dịch vụ công nghệ thông tin, đơn vị chủ trì thuê dịch vụ lập hồ sơ đề xuất cấp độ; Đối với các hệ thống thông tin đang trong giai đoạn triển khai, đơn vị chủ trì triển khai lập hồ sơ đề xuất cấp độ; Đối với các hệ thống thông tin đang vận hành, đơn vị vận hành lập hồ sơ đề xuất cấp độ.

b) Đối với các hệ thống thông tin được đề xuất từ cấp độ 3 trở lên, đơn vị chuyên trách về an toàn thông tin của các đơn vị thuộc, trực thuộc Bộ cần gửi xin ý kiến chuyên môn của Cục Khoa học công nghệ và Đào tạo trước khi trình các cấp có thẩm quyền thẩm định, phê duyệt cấp độ.

c) Thẩm quyền thẩm định và phê duyệt cấp độ theo quy định tại điểm b, Khoản 1, Điều 12 của Thông tư số 12/2022/TT-BTTTT.

6. Trình tự, thủ tục xác định cấp độ hệ thống thông tin

a) Việc xác định, phân loại hệ thống thông tin theo quy định tại Điều 7 Thông tư số 12/2022/TT-BTTTT.

b) Nội dung của hồ sơ đề xuất cấp độ hệ thống thông tin theo quy định tại Điều 15 Nghị định 85/2016/NĐ-CP.

d) Nội dung, thời gian thẩm định hồ sơ đề xuất cấp độ hệ thống thông tin quy định tại Điều 16 Nghị định 85/2016/NĐ-CP.

e) Trình tự, thủ tục xác định cấp độ hệ thống thông tin theo quy định tại Điều 13, Điều 14 Nghị định 85/2016/NĐ-CP.

7. Phương án bảo đảm an toàn hệ thống thông tin

a) Phương án bảo đảm an toàn hệ thống thông tin phải phù hợp với cấp độ của hệ thống thông tin và đáp ứng yêu cầu quy định tại Thông tư số 12/2022/TT-BTTTT, phù hợp với tiêu chuẩn TCVN 11930:2017, các tiêu chuẩn, quy chuẩn kỹ thuật khác và chính sách an toàn thông tin mạng của Bộ Y tế, chính sách an toàn thông tin mạng của các đơn vị thuộc, trực thuộc Bộ (nếu có).

b) Chủ quản hệ thống thông tin hoặc đơn vị được ủy quyền quản lý trực tiếp hệ thống thông tin tổ chức triển khai phương án bảo đảm an toàn hệ thống thông tin sau khi hồ sơ đề xuất cấp độ hoặc phương án bảo đảm an toàn hệ thống được phê duyệt.

c) Đơn vị/bộ phận chuyên trách về an toàn thông tin thuộc đơn vị chịu trách nhiệm giám sát việc triển khai các phương án bảo đảm an toàn thông tin đã được phê duyệt.

2. Phương án phương án bảo đảm an toàn thông tin, an ninh mạng hệ thống thông tin phải phù hợp với cấp độ của hệ thống thông tin và đáp ứng yêu cầu quy định tại Nghị định số 85/2016/NĐ-CP, Điều 24, Điều 25 của Nghị định số 53/2022/NĐ-CP, Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông, đáp ứng tiêu chuẩn TCVN 11930:2017 và quy định về an toàn thông tin mạng của Bộ.

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

1. Các hệ thống thông tin phải được thực hiện giám sát an toàn thông tin, an ninh mạng.

2. Đơn vị vận hành hệ thống thông tin có trách nhiệm phối hợp với Trung tâm Thông tin y tế Quốc gia tổ chức thực hiện việc giám sát hệ thống thông tin theo Điều 15 của Nghị định số 53/2022/NĐ-CP và Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông về quy định hoạt động giám sát an toàn hệ thống thông tin.

3. Đối với hệ thống thông tin quan trọng về an ninh quốc gia, thực hiện giám sát an ninh mạng theo Điều 14 Luật An ninh mạng.

Điều 13. Ứng cứu sự cố an toàn hệ thống thông tin

1. Đơn vị chuyên trách ứng cứu khẩn cấp sự cố an toàn thông tin mạng:

a) Trung tâm Thông tin Y tế Quốc gia là đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng của Bộ. Đơn vị/bộ phận chuyên trách về an toàn thông tin mạng tại các đơn vị thuộc, trực thuộc Bộ đảm nhiệm vai trò chuyên trách về ứng cứu sự cố an toàn thông tin mạng trong phạm vi quản lý công nghệ thông tin của đơn vị. Đơn vị/bộ phận chuyên trách về ứng cứu sự cố an toàn thông tin mạng thực hiện trách nhiệm quy định tại khoản 2 Điều 6 Quyết định số 05/2017/QĐ-TTg.

c) Bộ thành lập Đội ứng cứu an toàn thông tin mạng của Bộ và tổ chức ứng cứu sự cố trong phạm vi của Bộ quản lý.

2. Kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng

a) Các đơn vị thuộc, trực thuộc Bộ tổ chức xây dựng, phê duyệt kế hoạch ứng phó sự cố cho các hệ thống thông tin do đơn vị trực tiếp quản lý theo đề cương tại Phụ lục II Quyết định số 05/2017/QĐ-TTg (bao gồm các điều chỉnh do Bộ Thông tin và Truyền thông ban hành nếu có) và tổ chức triển khai kế hoạch sau khi phê duyệt.

b) Các kế hoạch ứng phó sự cố sau khi được phê duyệt phải gửi Trung tâm Thông tin Y tế Quốc gia và Cục Khoa học công nghệ và Đào tạo tổng hợp thành kế hoạch chung của Bộ.

3. Quy trình ứng cứu sự cố an toàn thông tin mạng

a) Các tổ chức, cá nhân khi phát hiện dấu hiệu tấn công hoặc sự cố an toàn thông tin mạng cần nhanh chóng báo cho đơn vị vận hành hệ thống thông tin, đơn vị chủ quản hệ thống thông tin liên quan, Trung tâm Thông tin Y tế Quốc gia. Trung tâm Thông tin Y tế Quốc gia có trách nhiệm cập nhật, công khai thông tin liên lạc, đường dây nóng của các đơn vị/bộ phận tiếp nhận thông tin sự cố của Bộ.

b) Khi xảy ra sự cố an toàn thông tin 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 và Điều 9 Thông tư 20/2017/TT-BTTTT, đồng thời báo cáo Trung tâm Thông tin Y tế Quốc gia để tổng hợp, báo cáo Lãnh đạo Bộ. Trách nhiệm của các đơn vị khi phát hiện, tiếp nhận xác minh, xử lý ban đầu và phân loại sự cố an toàn thông tin mạng theo quy định tại Điều 12 Quyết định 05/2017/QĐ-TTg và Điều 10 Thông tư số 20/2017/TT-BTTTT.

c) Quy trình ứng cứu sự cố an toàn thông tin mạng theo quy định tại Điều

13, Điều 14 Quyết định số 05/2017/QĐ-TTg và Điều 11 Thông tư số 20/2017/TT-BTTTT.

4. Diễn tập ứng cứu sự cố an toàn thông tin mạng

a) Chủ quản hệ thống thông tin tổ chức diễn tập ứng cứu sự cố theo kế hoạch ứng phó sự cố được phê duyệt.

b) Trung tâm Thông tin Y tế Quốc gia chủ trì, phối hợp với các đơn vị trực thuộc Bộ tham gia các cuộc diễn tập quốc gia, quốc tế do Cơ quan điều phối quốc gia, Bộ Thông tin và Truyền thông tổ chức và tổ chức diễn tập ứng cứu sự cố trong phạm vi Bộ theo tần suất quy định tại điểm b Nhiệm vụ 4 mục II Điều 1 Quyết định số 1622/QĐ-TTg ngày 25/10/2017 của Thủ tướng Chính phủ.

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

1. Chủ quản hệ thống thông tin có thẩm quyền yêu cầu kiểm tra, đánh giá đối với các hệ thống thông tin thuộc thẩm quyền quản lý. Đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin có thẩm quyền yêu cầu kiểm tra, đánh giá đối với các hệ thống thông tin do đơn vị này phê duyệt hồ sơ đề xuất cấp độ.

2. Đơn vị chủ trì kiểm tra, đánh giá là đơn vị được cấp có thẩm quyền giao nhiệm vụ hoặc được lựa chọn để thực hiện việc kiểm tra, đánh giá. Đối tượng kiểm tra, đánh giá là chủ quản hệ thống thông tin hoặc đơn vị vận hành hệ thống thông tin và các hệ thống thông tin có liên quan.

3. Nội dung, hình thức kiểm tra, đánh giá theo quy định tại Điều 11 Thông tư số 12/2022/TT-BTTTT.

4. Cục Khoa học công nghệ và Đào tạo thực hiện việc kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ tại Bộ theo quy định tại Điều 12 Thông tư số 12/2022/TT-BTTTT.

5. Cục Khoa học công nghệ và Đào tạo, đơn vị chuyên trách về an toàn thông tin của các đơn vị thuộc, trực thuộc Bộ thực hiện việc đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin theo thẩm quyền. Nội dung đánh giá là cơ sở để điều chỉnh phương án bảo đảm an toàn thông tin cho phù hợp.

Điều 15. Đào tạo, bồi dưỡng nghiệp vụ, tuyên truyền, phổ biến nâng cao nhận thức về an toàn thông tin mạng

1. Các đơn vị thuộc, trực thuộc Bộ xác định nhu cầu về đào tạo cho nguồn nhân lực để bảo đảm an toàn thông tin tại đơn vị mình gửi Cục Khóc công nghệ và Đào tạo tổng hợp.

2. Các đơn vị thuộc, trực thuộc Bộ tổ chức đào tạo, bồi dưỡng nghiệp vụ về an toàn thông tin cho cán bộ công nghệ thông tin, cán bộ chuyên trách an

toàn thông tin mạng các đơn vị trực thuộc; đào tạo cơ bản về an toàn thông tin cho cán bộ quản lý, người sử dụng máy tính thuộc đơn vị.

3. Các đơn vị thuộc, trực thuộc Bộ phải thường xuyên tổ chức các hoạt động tuyên truyền, phổ biến nâng cao nhận thức về bảo đảm an toàn, an ninh thông tin mạng đến toàn thể bộ cán bộ, công chức, viên chức và người lao động tại đơn vị.

Chương III TỔ CHỨC THỰC HIỆN

Điều 16. Trách nhiệm của Cục Khoa học Công nghệ và Đào tạo

1. Chủ trì, phối hợp với cơ quan, đơn vị liên quan đề hướng dẫn, theo dõi, đôn đốc, kiểm tra và đánh giá việc thực hiện Quy chế này.

2. Là đơn vị chuyên trách về an toàn thông tin, an ninh mạng của Bộ, chủ trì phối hợp với Trung tâm Thông tin y tế Quốc gia tổ chức thẩm định, trình Lãnh đạo Bộ phê duyệt hồ sơ đề xuất cấp độ, thẩm định phương án bảo đảm an toàn thông tin theo cấp độ cho các hệ thống thông tin trong phạm vi quản lý của Bộ theo quy định.

3. Phối hợp với Trung tâm Thông tin y tế Quốc gia giám sát, kiểm tra, đánh giá việc triển khai các phương án bảo đảm an toàn thông tin, an ninh mạng đã được phê duyệt đối với các hệ thống thông tin trong phạm vi quản lý của Bộ.

4. Phối hợp với Trung tâm Thông tin y tế Quốc gia và các cơ quan, đơn vị liên quan để tham mưu cho Lãnh đạo Bộ Y tế thành lập Đội ứng cứu sự cố an toàn thông tin mạng của Bộ Y tế; xây dựng và trình lãnh đạo Bộ ban hành Kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng ngành y tế.

5. Tổng hợp nhu cầu của các đơn vị thuộc, trực thuộc Bộ và gửi Vụ Kế hoạch - Tài chính để đề xuất dự toán kinh phí cho các hoạt động bảo đảm an toàn, an ninh thông tin mạng.

6. Xây dựng và trình Bộ kế hoạch tuyên truyền, phổ biến nâng cao nhận thức về an toàn, an ninh thông tin mạng tại Bộ Y tế và thực hiện các nội dung theo kế hoạch đã được phê duyệt.

Điều 17. Trách nhiệm của Trung tâm Thông tin y tế Quốc gia

1. Tổ chức triển khai các quy định bảo đảm an toàn thông tin, an ninh mạng của Bộ theo phân công tại Quy chế này.

2. Là đơn vị chuyên trách về tiếp nhận thông báo sự cố, ứng cứu sự cố an toàn thông tin, an ninh mạng của Bộ, thực hiện trách nhiệm quy định tại Khoản 2 Điều 6 Quyết định số 05/2017/QĐ-TTg ngày 16/03/2017 của Thủ tướng

Chính phủ. Chủ trì, phối hợp với Cục Khoa học công nghệ và Đào tạo và các cơ quan, đơn vị liên quan có trách nhiệm xây dựng và trình lãnh đạo Bộ ban hành Kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng ngành y tế.

3. Phối hợp với Cục Khoa học công nghệ và Đào tạo tổ chức thẩm định, trình Lãnh đạo Bộ phê duyệt hồ sơ đề xuất cấp độ, thẩm định phương án bảo đảm an toàn thông tin theo cấp độ cho các hệ thống thông tin trong phạm vi quản lý của Bộ theo quy định

4. Phối hợp với Cục Khoa học công nghệ và Đào tạo tham mưu thành lập Đội ứng cứu sự cố an toàn thông tin mạng của Bộ Y tế.

5. Chịu trách nhiệm bảo đảm an toàn thông tin, an ninh mạng cho các hệ thống thông tin dùng chung của Bộ. Hỗ trợ các đơn vị, cá nhân về công tác bảo đảm an toàn thông tin, an ninh mạng.

6. Chủ trì, phối hợp với các đơn vị thuộc và trực thuộc Bộ để tổ chức, tham gia các cuộc diễn tập quốc gia, quốc tế do Cơ quan điều phối quốc gia về ứng cứu sự cố an toàn thông tin; hàng năm tổ chức diễn tập ứng cứu sự cố an toàn thông tin mạng trong phạm vi của Bộ theo Quyết định số 1622/QĐ-TTg ngày 25/10/2017 của Thủ tướng Chính phủ.

6. Phối hợp với Cục Khoa học công nghệ và Đào tạo tổ chức các khóa tập huấn, đào tạo về an toàn thông tin, an ninh mạng cho cán bộ, công chức, viên chức, người lao động của Bộ.

Điều 18. Trách nhiệm của Vụ Kế hoạch – Tài chính

1. Tổ chức triển khai các quy định bảo đảm an toàn thông tin, an ninh mạng của Bộ theo phân công tại Quy chế này.

2. Chủ trì, phối hợp với Cục Khoa học công nghệ và Đào tạo để đề xuất và báo cáo Lãnh đạo Bộ phê duyệt dự toán kinh phí hằng năm cho các hoạt động bảo đảm an toàn, an ninh thông tin mạng của các đơn vị thuộc, trực thuộc Bộ.

Điều 19. Trách nhiệm của các đơn vị thuộc và trực thuộc Bộ

1. Tổ chức phổ biến, đảm bảo việc tuân thủ Quy chế này và các quy định của Nhà nước về an toàn thông tin, an ninh mạng đối với các cá nhân, tập thể thuộc đơn vị mình.

2. Lập hồ sơ đề xuất cấp độ an toàn thông tin cho các hệ thống thông tin (nếu có) tại đơn vị và báo cáo với Cục Khoa học công nghệ và Đào tạo để thẩm định phương án bảo đảm an toàn thông tin theo cấp độ cho các hệ thống thông tin theo quy định.

3. Thường xuyên kiểm tra, đôn đốc việc triển khai an toàn thông tin, an ninh mạng trong công việc của các cá nhân, tập thể do đơn vị quản lý.

4. Đơn vị chủ trì xây dựng hệ thống thông tin (nếu có) khi bàn giao hệ thống thông tin về Trung tâm Thông tin y tế Quốc gia vận hành phải bàn giao đầy đủ hồ sơ xây dựng hệ thống theo quy định, trong đó có hồ sơ về an toàn thông tin gồm: hồ sơ thiết kế, hồ sơ kiểm thử, hồ sơ đề xuất cấp độ an toàn thông tin và nhật ký vận hành hệ thống thông tin tới thời điểm bàn giao để phục vụ việc kiểm tra, đánh giá an toàn thông tin hệ thống trước khi đưa vào vận hành chính thức.

5. Có trách nhiệm tổ chức triển khai phương án bảo đảm an toàn hệ thống thông tin sau khi được phê duyệt; tổ chức, triển khai, tham gia diễn tập ứng cứu sự cố theo kế hoạch ứng phó sự cố đã được Bộ phê duyệt.

6. Thực hiện các báo cáo định kỳ hoặc theo yêu cầu gửi Cục Khoa học Công nghệ và Đào tạo và Trung tâm Thông tin y tế Quốc gia để tổng hợp, báo cáo Bộ Y tế và các cơ quan có thẩm quyền.

Điều 20. Trách nhiệm của các cơ quan, tổ chức có kết nối vào hệ thống mạng của Bộ và cơ quan, tổ chức cung cấp dịch vụ công nghệ thông tin, an toàn thông tin, an ninh mạng cho các đơn vị thuộc, trực thuộc Bộ

1. Thực hiện trách nhiệm theo quy định tại Quy chế này và các nhiệm vụ do chủ quản hệ thống thông tin phân công.

2. Chỉ đạo, phân công các bộ phận kỹ thuật thuộc đơn vị (quản lý ứng dụng; quản lý dữ liệu; vận hành hệ thống thông tin; triển khai và hỗ trợ kỹ thuật) triển khai công tác bảo đảm an toàn thông tin trong tất cả các công đoạn liên quan đến hệ thống thông tin.

3. Phối hợp với Trung tâm Thông tin y tế Quốc gia rà soát, đánh giá các phương án bảo đảm an toàn thông tin trong quá trình vận hành, sử dụng các hệ thống thông tin, máy chủ, thiết bị công nghệ thông tin của mình có kết nối với các hệ thống thông tin của chủ quản hệ thống thông tin.

4. Thông báo sự cố hoặc các hành vi phá hoại, xâm nhập về Cục Khoa học Công nghệ và Đào tạo, Trung tâm Thông tin y tế Quốc gia để xem xét, hỗ trợ, điều phối và xử lý.

Điều 21. Trách nhiệm của cá nhân

1. Thực hiện các quy định liên quan tại Quy chế này về bảo đảm an toàn thông tin, an ninh mạng.

2. Tham gia đầy đủ các lớp đào tạo ngắn hạn, các hội thảo, hội nghị phổ biến, nâng cao nhận thức, diễn tập an toàn thông tin và ứng cứu sự cố để bảo đảm an toàn thông tin, an ninh mạng.

3. Chịu trách nhiệm về các vi phạm làm mất an toàn thông tin, an ninh mạng do không tuân thủ Quy chế này.

Điều 22. Kinh phí thực hiện

1. Kinh phí bảo đảm an toàn thông tin, an ninh mạng được bố trí từ nguồn ngân sách nhà nước và các nguồn kinh phí hợp pháp khác.

2. Căn cứ vào kế hoạch hàng năm, các đơn vị liên quan có trách nhiệm xây dựng kế hoạch, đề xuất dự toán cho các hoạt động bảo đảm an toàn, an ninh thông tin mạng gửi Cục Khoa học công nghệ và Đào tạo, Vụ Kế hoạch - Tài chính tổng hợp, trình Bộ phê duyệt.

Điều 23. Công tác kiểm tra

1. Các đơn vị thuộc, trực thuộc Bộ phải thường xuyên kiểm tra, theo dõi và đánh giá công tác bảo đảm an toàn, an ninh thông tin mạng tại cơ quan, đơn vị mình, coi đây là nhiệm vụ trọng tâm của đơn vị.

2. Giao Cục Khoa học công nghệ và Đào tạo kiểm tra và báo cáo Bộ việc thực hiện Quy chế này tại các đơn vị thuộc, trực thuộc Bộ.

Điều 24. Chế độ, nội dung báo cáo

Quy định về chế độ báo cáo và nội dung báo cáo được quy định tại Điều 13, Điều 14 của Thông tư số 12/2022/TT-BTTTT.

Điều 25. Trách nhiệm thi hành

1. Quy chế này có hiệu lực từ ngày ký, ban hành.

2. Thủ trưởng các đơn vị thuộc và trực thuộc Bộ có trách nhiệm triển khai thực hiện, phổ biến, quán triệt đến toàn bộ cán bộ, công chức, viên chức, người lao động trong đơn vị Quy chế này; thường xuyên kiểm tra việc thực hiện Quy chế tại đơn vị; chịu trách nhiệm trước pháp luật và trước Bộ trưởng Bộ Y tế về các vi phạm, thất thoát thông tin, dữ liệu thuộc phạm vi quản lý của đơn vị.

3. Trong quá trình thực hiện, nếu có những vấn đề khó khăn, vướng mắc, các đơn vị phản ánh về Cục Khoa học công nghệ và Đào tạo để tổng hợp, trình Bộ trưởng xem xét, sửa đổi, bổ sung Quy chế này./.