BỘ GIÁO DỤC VÀ ĐÀO TẠO -------	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc ----------
Số: 3238/QĐ-BGDĐT	*Hà Nội, ngày 30 tháng 10 năm 2024*

QUYẾT ĐỊNH

BAN HÀNH QUY CHẾ QUẢN LÝ VÀ SỬ DỤNG MẠNG MÁY TÍNH ĐẢM BẢO AN NINH MẠNG CỦA BỘ GIÁO DỤC VÀ ĐÀO TẠO

BỘ TRƯỞNG BỘ GIÁO DỤC VÀ ĐÀO TẠO

Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19 tháng 11 năm 2015;

Căn cứ Luật An ninh mạng số 24/2018/QH14 ngày 12 tháng 6 năm 2018;

Căn cứ Nghị định số 86/2022/NĐ-CP ngày 16 tháng 8 năm 2022 của Chính phủ Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Giáo dục và Đào tạo;

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 53/2022/NĐ-CP ngày 15 tháng 8 năm 2022 của Chính phủ về việc 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 Chỉ thị 14/CT-TTg ngày 25 tháng 5 năm 2028 của Thủ tướng Chính phủ về việc nâng cao năng lực phòng, chống phần mềm độc hại;

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 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 Công nghệ thông tin.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế quản lý và sử dụng mạng máy tính đảm bảo an ninh mạng của Bộ Giáo dục và Đào tạo.

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày ký.

Điều 3. Chánh Văn phòng, Cục trưởng Cục Công nghệ thông tin và thủ trưởng các đơn vị thuộc Bộ Giáo dục và Đào tạo và tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Nơi nhận:
- Như Điều 3;
- Bộ trưởng (để b/c);
- Các Thứ trưởng;
- Các đơn vị thuộc Bộ;
- Cổng thông tin điện tử Bộ;
- Lưu: VT, CNTT.

Hoàng Minh Sơn

QUY CHẾ

QUẢN LÝ VÀ SỬ DỤNG MẠNG MÁY TÍNH ĐẢM BẢO AN NINH MẠNG CỦA BỘ GIÁO DỤC VÀ ĐÀO TẠO

(Ban hành kèm theo Quyết định số 3238/QĐ-BGDĐT ngày 30 tháng 10 năm 2024 của Bộ trưởng Bộ Giáo dục và Đào tạo)

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 quản lý và sử dụng mạng máy tính nội bộ, mạng máy tính có kết nối mạng Internet và mạng truyền số liệu chuyên dùng trong các hoạt động chuyển đổi số, ứng dụng công nghệ thông tin, thuộc phạm vi quản lý của Bộ Giáo dục và Đào tạo.

2. Đối tượng áp dụng:

a) Các đơn vị thuộc Bộ Giáo dục và Đào tạo (sau đây gọi là đơn vị) và công chức, viên chức và người lao động trong đơn vị (sau đây gọi là cá nhân);

b) Cơ quan, tổ chức, cá nhân có kết nối vào hệ thống thông tin của Bộ Giáo dục và Đào tạo;

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 Bộ Giáo dục và Đào tạo.

Điều 2. Giải thích từ ngữ

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

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

2. *An ninh mạng* là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

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

4. *Trung tâm dữ liệu* là một cơ sở vật lý dùng để chứa các hệ thống máy chủ, thiết bị mạng, lưu trữ, và các tài nguyên công nghệ khác, nhằm quản lý, lưu trữ, và xử lý dữ liệu. Trung tâm dữ liệu của Bộ Giáo dục và Đào tạo bao gồm khu vực hạ tầng thuê bên ngoài (các nhà cung cấp dịch vụ) và Phòng máy chủ đặt tại trụ sở cơ quan Bộ.

5. *Chủ quản hệ thống thông tin* là cơ quan, tổ chức có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin. Bộ Giáo dục Đào tạo là Chủ quản các hệ thống thông tin do Bộ trưởng Bộ Giáo dục và Đào tạo quyết định chủ trương đầu tư sử dụng tại cơ quan Bộ.

6. *Đơn vị quản lý hệ thống thông tin* là đơn vị được Bộ trưởng Bộ Giáo dục và Đào tạo giao trực tiếp quản lý, khai thác sử dụng hệ thống thông tin phục vụ chuyên môn nghiệp vụ của đơn vị.

7. *Đơn vị vận hành hệ thống thông tin* là đơn vị được Bộ trưởng Bộ Giáo dục và Đào tạo giao vận hành kỹ thuật hệ thống thông tin đảm bảo hoạt động ổn định.

8. *Đơn vị chuyên trách an toàn thông tin, an ninh mạng* là đơn vị có chức năng, nhiệm vụ bảo đảm an toàn thông tin của chủ quản hệ thống thông tin (theo Khoản 5 Điều 3 Nghị định 85/2016/NĐ-CP về bảo đảm an toàn hệ thống thông tin theo cấp độ); Đơn vị phụ trách về ứng cứu sự cố an toàn thông tin mạng (theo Quyết định số 05/2017/QĐ-TTg ngày 16/03/2017 của Thủ tướng Chính phủ về hệ thống phương án ứng cứu khẩn cấp đảm bảo an toàn thông tin mạng quốc gia).

9. *Thiết bị xử lý thông tin* là thiết bị dùng để tạo lập, xử lý, lưu trữ, truyền đưa thông tin dưới dạng điện tử (máy tính, máy in, điện thoại thông minh, thiết bị mạng, thiết bị an ninh mạng, camera giám sát và các thiết bị tương tự khác).

10. *Mạng máy tính nội bộ* là một hệ thống mạng bao gồm hệ thống các máy tính và các thiết bị ngoại vi được kết nối với nhau trong phạm vi hẹp, thông qua các thiết bị mạng để chia sẻ tài nguyên như thông tin, dữ liệu, phần mềm và các thiết bị ngoại vi.

11. *Mạng máy tính kết nối Internet* được hiểu là hệ thống mạng máy tính được kết nối dịch vụ mạng máy tính toàn cầu.

12. *Mạng máy tính chuyên dùng* (máy tính, thiết bị lưu trữ, máy in...) được hiểu là mạng máy tính sử dụng xử lý thông tin bí mật nhà nước, được tách biệt vật lý hoàn toàn với mạng máy tính kết nối Internet và mạng máy tính nội bộ.

13. *Mã độc* là đoạn mã chương trình hoặc phần mềm độc hại được tạo ra nhằm xâm nhập, gây thiệt hại, hoặc lấy cắp thông tin từ các thiết bị và hệ thống máy tính mà không có sự cho phép của người dùng.

14. *Dữ liệu nhạy cảm* là dữ liệu nếu lộ lọt thông tin sẽ gây ảnh hưởng xấu đến cá nhân, tổ chức. Dữ liệu nhạy cảm cá nhân được quy định tại khoản 4 Điều 2 Nghị định 13/2023/NĐ-CP; Dữ liệu nhạy cảm tổ chức là dữ liệu thông tin lưu hành nội bộ của đơn vị hoặc do đơn vị quản lý, nếu lộ lọt ra ngoài sẽ gây ảnh hưởng xấu đến danh tiếng, tài chính, tổ chức và hoạt động của đơn vị.

Điều 3. Nguyên tắc chung

1. Quản lý và khai thác mạng máy tính của Bộ Giáo dục và Đào tạo nhằm đảm bảo sự ổn định, thống nhất, hỗ trợ tốt nhất việc khai thác, sử dụng các hệ thống thông tin trong cơ quan Bộ. Công tác bảo đảm an toàn thông tin và an ninh mạng phải được thực hiện xuyên suốt, đồng bộ với quá trình mua sắm, nâng cấp, vận hành, bảo trì và ngừng sử dụng hạ tầng, hệ thống thông tin, phần mềm, dữ liệu.

2. Bảo đảm an toàn thông tin và đảm bảo an ninh mạng phải gắn với trách nhiệm của người đứng đầu cơ quan, đơn vị và cá nhân trực tiếp liên quan.

3. Trường hợp có văn bản, quy định cập nhật, thay thế hoặc quy định khác tại văn bản quy phạm pháp luật, quyết định của cấp có thẩm quyền cao hơn thì áp dụng quy định tại văn bản đó.

4. Thông tin thuộc Danh mục bí mật nhà nước được bảo vệ theo quy định của pháp luật về bảo vệ bí mật nhà nước.

5. Xử lý sự cố an toàn thông tin và 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. Các hành vi bị nghiêm cấm quy định tại Điều 7 Luật An toàn thông tin mạng năm 2015 và Điều 8 Luật An ninh mạng năm 2018.

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 mà không có sự hướng dẫn hoặc đồng ý của đơn vị vận hành hệ thống mạng nội bộ.

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

4. Cố ý tạo lập, cài đặt, phát tán mã độc gây ảnh hưởng đến hoạt động bình thường của hệ thống thông tin.

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, sử dụng trái phép 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 khi trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

Chương II

QUẢN LÝ, SỬ DỤNG MẠNG MÁY TÍNH

Điều 5. Đối với Trung tâm dữ liệu của Bộ

1. Cục Công nghệ thông tin có trách nhiệm:

a) Thiết lập khu vực hạn chế tiếp cận, chỉ những cá nhân có quyền, nhiệm vụ theo quy định của thủ trưởng cơ quan, đơn vị mới được phép vào trung tâm dữ liệu. Quá trình vào, ra phòng máy chủ phải được ghi nhận vào nhật ký quản lý trung tâm dữ liệu.

b) Tham mưu phương án đảm bảo hệ thống lưu điện, điện máy nổ đủ công suất và duy trì thời gian hoạt động của phòng máy chủ ít nhất 3 tiếng đồng hồ từ khi có sự cố mất điện lưới.

c) Thiết lập cơ chế bảo vệ cho 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; thường xuyên theo dõi phát hiện xâm nhập và biện pháp kiểm soát truy nhập, kết nối vật lý phù hợp với từng khu vực.

d) Xây dựng nội quy hoặc hướng dẫn làm việc tại khu vực Trung tâm dữ liệu; phân công cán bộ thường xuyên giám sát thiết bị, hạ tầng của trung tâm dữ liệu.

2. Đơn vị Quản lý hệ thống thông tin sử dụng hạ tầng công nghệ thông tin trong Trung tâm dữ liệu của Bộ có trách nhiệm xây dựng quy chế phối hợp với Cục Công nghệ thông tin quản lý vận hành hệ thống; phân công đầu mối chịu trách nhiệm đối với hệ thống thông tin; tổ chức vận hành và đảm bảo an toàn, an ninh thông tin cho hệ thống thông tin của đơn vị mình.

Điều 6. Đối với Hệ thống mạng nội bộ

1. Cục Công nghệ thông tin là đơn vị quản lý mạng nội bộ của cơ quan Bộ, đảm bảo:

a) Mạng nội bộ được thiết kế phân vùng theo chức năng cơ bản (theo các chính sách an toàn thông tin riêng), bao gồm: vùng mạng người dùng; vùng mạng kết nối Internet và các mạng khác (nếu có); vùng mạng máy chủ công cộng; vùng mạng máy chủ nội bộ; vùng mạng quản trị.

b) Tổ chức giám sát dữ liệu trao đổi giữa các vùng mạng, việc giám sát thực hiện bởi hệ thống các thiết bị bảo mật và giám sát an toàn, an ninh thông tin; Thiết lập, cấu hình các tính năng theo thiết kế của các trang thiết bị bảo mật mạng; thực hiện các biện pháp, giải pháp để dò tìm và phát hiện kịp thời các điểm yếu, lỗ hổng về mặt kỹ thuật của hệ thống mạng; thường xuyên kiểm tra, phát hiện những kết nối, trang thiết bị, phần mềm cài đặt bất hợp pháp vào mạng.

2. Các đơn vị, tổ chức, cá nhân tham gia sử dụng mạng nội bộ có trách nhiệm:

a) Không tiết lộ thiết kế, thông số cấu hình hệ thống mạng nội bộ cho tổ chức, cá nhân khác; Không được phép truy cập bất hợp pháp vào các khu vực không được cấp quyền.

b) Không được tự ý thay đổi những thông số mạng hay tự ý đưa các thiết bị mạng, thiết bị viễn thông khác tham gia kết nối vào hệ thống mạng.

c) Các cơ quan bên ngoài khi có kết nối trực tiếp trang thiết bị vào hệ thống mạng của Bộ Giáo dục và Đào tạo với mục đích phục vụ công việc, phải được sự đồng ý bằng văn bản của Cục Công nghệ thông tin và tuân theo các quy định, các tiêu chuẩn kỹ thuật phù hợp với hệ thống mạng của Bộ Giáo dục và Đào tạo.

Điều 7. Đối với Hệ thống mạng kết nối Internet

1. Cục Công nghệ thông tin có trách nhiệm áp dụng các biện pháp kỹ thuật cần thiết bảo đảm an toàn thông tin trong hoạt động kết nối Internet, tối thiểu đáp ứng các yêu cầu sau: có hệ thống tường lửa và hệ thống bảo vệ các vùng truy nhập Internet, đáp ứng nhu cầu kết nối đồng thời, hỗ trợ các công nghệ mạng riêng ảo (VPN) thông dụng, có phần cứng mã hóa tích hợp để tăng tốc độ mã hóa dữ liệu, có khả năng bảo vệ hệ thống trước các loại tấn công từ chối dịch vụ (DDoS); Lọc bỏ, không cho phép truy nhập các trang tin có nghi ngờ chứa mã độc hoặc các nội dung không phù hợp.

2. Đơn vị quản lý hệ thống thông tin sử dụng hạ tầng tại Trung tâm dữ liệu của Bộ có trách nhiệm phối hợp với Cục Công nghệ thông tin từ bước thiết kế hệ thống, kiểm tra và rà soát về an toàn thông tin đáp ứng theo yêu cầu về an toàn theo cấp độ quy định tại Nghị định số 85/2016/NĐ-CP trước khi đưa hệ thống vào sử dụng. Các hệ thống thông tin cài đặt trong Trung tâm dữ liệu của Bộ phải được kiểm tra đảm bảo an toàn thông tin và tuân thủ Kiến trúc Chính phủ điện tử của Bộ Giáo dục và Đào tạo.

3. Đối với các cá nhân có liên quan:

a) Đơn vị quản lý hệ thống thông tin sử dụng hạ tầng tại Trung tâm dữ liệu của Bộ có trách nhiệm gửi danh sách cá nhân được giao quản trị các hệ thống thông tin cho Cục Công nghệ thông tin để quản lý và cấp tài khoản truy cập hệ thống qua mạng riêng ảo (VPN).

b) Cá nhân sử dụng mạng máy tính có kết nối Internet, sử dụng tài khoản truy cập hệ thống qua mạng riêng ảo phải tuân thủ quy định tại Quy chế này. Khi phát hiện các nguy cơ mất an toàn, an ninh mạng, kịp thời thông báo cho Cục Công nghệ thông tin để xử lý.

Điều 8. Đối với Hệ thống mạng máy tính chuyên dùng phục vụ công tác bí mật nhà nước (BMNN)

1. Thủ trưởng các đơn vị thuộc Bộ Giáo dục và Đào tạo có trách nhiệm chỉ đạo, kiểm tra đôn đốc việc thực hiện quy định của pháp luật và nội quy, quy chế về máy tính chuyên dùng bảo vệ bí mật nhà nước:

a) Máy tính chuyên dùng, thiết bị phục vụ công tác bảo vệ BMNN tại đơn vị phải được bàn giao, phân công cụ thể cho các cá nhân đầu mối quản lý, sử dụng.

b) Các máy tính và thiết bị phải được đơn vị phụ trách mạng chuyên dùng, đơn vị phụ trách bí mật nhà nước kiểm tra về an toàn, an ninh trước khi đưa vào sử dụng.

c) Máy tính khi kết nối mạng chuyên dùng phải được đơn vị chuyên trách an toàn thông tin, an ninh mạng cài đặt và thiết lập cấu hình, trong quá trình sử dụng phải tuân thủ các quy định, không được tự ý thay đổi cấu hình kết nối.

d) Máy tính, thiết bị phục vụ công tác BMNN phải độc lập, không kết nối mạng với mạng nội bộ hoặc mạng có kết nối Internet; các cổng giao tiếp, thiết bị kết nối không dây (wifi, Bluetooth...) phải được vô hiệu hóa, dán niêm phong; các thiết bị ngoại vi lưu trữ phải sử dụng mã hóa do các đơn vị như Ban Cơ yếu Chính phủ cấp.

đ) Tổ chức thu hồi tài liệu, máy tính, thiết bị công nghệ thông tin có chứa BMNN khi người được phân công quản lý BMNN thôi việc, chuyển công tác, nghỉ hưu, từ trần hoặc vì lý do khác mà không được phân công tiếp tục quản lý.

2. Khi xảy ra lộ, mất BMNN thuộc phạm vi quản lý, cá nhân đầu mối của đơn vị cần kịp thời báo cáo với thủ trưởng đơn vị và thông báo với đơn vị phụ trách về BMNN, đồng thời, thông báo tới Cục Công nghệ thông tin để phối hợp xử lý đối với các sự việc liên quan tới an toàn thông tin, an ninh mạng.

Điều 9. Đối với các Hệ thống thông tin

Đơn vị quản lý hệ thông tin có trách nhiệm thiết lập, cấu hình an toàn thông tin theo đúng cấp độ của hệ thống; kiểm tra và giám sát thường xuyên và định kỳ để đảm bảo an toàn thông tin, an ninh mạng cho hạ tầng máy chủ và phần mềm, dịch vụ cài đặt trên máy chủ như sau:

1. Đối với hệ thống hạ tầng máy chủ của từng hệ thống thông tin

a) Phải được đặt trong các vùng mạng dành riêng cho máy chủ, tối thiểu gồm vùng mạng máy chủ công cộng, vùng mạng máy chủ nội bộ và vùng mạng máy chủ quản trị.

b) Chỉ cho phép kết nối đến những dịch vụ cần thiết trên Internet.

c) Chỉ mở và cung cấp các dịch vụ cần thiết ra Internet.

d) Chỉ cài đặt và sử dụng các phần mềm đúng bản quyền, nguồn gốc rõ ràng, thực sự cần thiết. Không sử dụng các phần mềm đã được cảnh báo không an toàn hoặc không được nhà sản xuất hỗ trợ kỹ thuật khi không thực sự cần thiết.

đ) Cài đặt các giải pháp phòng chống mã độc tập trung và phòng chống tấn công xâm nhập mạng phù hợp với yêu cầu theo từng cấp độ.

e) Triển khai các biện pháp sao lưu dự phòng để nâng cao khả năng phục hồi hoạt động khi xảy ra sự cố.

g) Giám sát thường xuyên, liên tục để phát hiện và cảnh báo sớm nguy cơ mất an toàn thông tin.

2. Đối với các phần mềm, dịch vụ cài đặt trên máy chủ

a) 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, dịch vụ.

b) Phần mềm, ứng dụng phải đáp ứng các yêu cầu: có tính năng xác thực người sử dụng; giới hạn số lần đăng nhập sai liên tiếp; giới hạn thời gian chờ đóng phiên kết nối; mã hóa thông tin xác thực trên hệ thống; không khuyến khích việc đăng nhập tự động.

c) 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.

d) Chỉ cho phép sử dụng các giao thức mạng có hỗ trợ chức năng mã hóa thông tin như SSL (Secure Sockets Layer), mạng riêng ảo 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.

đ) 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 kết nối, tài khoản (nếu có), nội dung truy cập dữ liệu và sử dụng phần mềm, ứng dụng, dịch vụ; các lỗi phát sinh trong quá trình hoạt động; thông tin đăng nhập khi quản trị, thông tin thay đổi cấu hình máy chủ.

e) 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. Định kỳ thực hiện quy trình

kiểm soát cài đặt, cập nhật, vá lỗi bảo mật phần mềm, ứng dụng và hệ điều hành trên các máy chủ.

Điều 10. Đối với dữ liệu và các cơ sở dữ liệu

Đơn vị quản lý, vận hành hệ thống thông tin có trách nhiệm:

1. Thực hiện bảo vệ thông tin, dữ liệu liên quan đến hoạt động công vụ, thông tin có nội dung quan trọng, nhạy cảm, dữ liệu cá nhân 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 và tuân thủ theo các quy định về bảo vệ dữ liệu cá nhân của Chính phủ.

2. 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.

3. 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.

4. Trang thiết bị công nghệ thông tin 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). Khi thanh lý thiết bị phải xóa nội dung dữ liệu lưu trữ bằng phần mềm, thiết bị hủy dữ liệu chuyên dụng hoặc phá hủy vật lý.

5. 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 11. Đối với hệ thống tài khoản sử dụng

1. Tài khoản truy cập hệ thống thông tin

a) Đơn vị quản lý hệ thống thông tin có trách nhiệm:

- Cấp tài khoản đúng thẩm quyền sử dụng cho các tổ chức, cá nhân sử dụng hệ thống thông tin và sử dụng tài khoản truy cập với định danh duy nhất gắn với cá nhân đó. Riêng đối với các hệ

thống thông tin dùng chung của Bộ sử dụng cơ chế đăng nhập một lần, chung một tài khoản truy nhập và mật khẩu do Cục Công nghệ thông tin cung cấp.

- Hệ thống tài khoản sử dụng phải được rà soát hàng năm, bảo đảm các tài khoản và quyền truy cập hệ thống được cấp phát đúng. Các tài khoản không sử dụng trong thời gian 01 năm phải bị khóa hoặc xóa bỏ (sau khi trao đổi, xác nhận với đơn vị sử dụng).

- Khi có yêu cầu khóa quyền truy cập hệ thống thông tin của tài khoản đang hoạt động, lãnh đạo đơn vị phải yêu cầu bằng văn bản gửi đơn vị Đơn vị quản lý hệ thống thông tin. Đơn vị quản lý hệ thống thông tin có quyền khóa quyền truy cập của tài khoản trong trường hợp tài khoản thực hiện các hành vi tấn công hoặc để xảy ra vấn đề mất an toàn, an ninh thông tin.

- Trường hợp người dùng thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ hưu thì đơn vị phải thông báo bằng văn bản cho đơn vị quản lý hệ thống thông tin để thực hiện điều chỉnh, thu hồi, hủy bỏ các quyền sử dụng của người dùng đó.

b) Các cá nhân sử dụng

- Có trách nhiệm bảo vệ thông tin tài khoản được cấp, không tiết lộ mật khẩu, không khuyến khích để chế độ lưu mật khẩu tự động hoặc đưa cho người khác phương tiện xác thực tài khoản của mình ngoại trừ các trường hợp: cần xử lý công việc khẩn cấp của đơn vị; cần cung cấp, bàn giao cho đơn vị các thông tin, tài liệu do cá nhân quản lý.

- Đổi ngay mật khẩu sau khi nhận bàn giao từ người khác hoặc có thông báo về sự cố an toàn thông tin, điểm yếu liên quan đến khả năng lộ mật khẩu.

2. Tài khoản quản trị hệ thống

Đơn vị quản lý, vận hành hệ thống thông tin có trách nhiệm:

a) Quản lý và cấp tài khoản quản trị hệ thống, tài khoản quản trị hệ thống phải tách biệt với tài khoản truy cập của người dùng thông thường. Tài khoản hệ thống phải được giao đích danh cá nhân làm công tác quản trị. Hạn chế dùng chung tài khoản quản trị.

b) Mật khẩu quản trị phải được quản lý trong các phần mềm mã hóa trên các thiết bị dành riêng cho quản trị hệ thống. Trường hợp cần thiết để bảo đảm an toàn, an ninh cho hệ thống, phải triển khai hệ thống quản lý tài khoản đặc quyền để thực hiện quản lý, lưu giữ, cấp phát tài khoản quản trị hệ thống.

c) Thiết bị (máy tính cá nhân, máy tính bảng, điện thoại...) phục vụ quản trị hệ thống, chỉ được sử dụng cho mục đích quản trị hệ thống, chỉ cài đặt và sử dụng các phần mềm quản trị đúng bản quyền, nguồn gốc rõ ràng, thực sự cần thiết, không được kết nối trực tiếp đến máy chủ để thực hiện quản trị cấu hình mà phải kết nối với máy chủ quản trị qua các đường truyền có mã hóa bảo mật theo quy định.

3. Quy định về mật khẩu của tài khoản

a) Độ dài mật khẩu tối thiểu 12 ký tự, trong đó có tối thiểu 3 trong 5 loại ký tự sau: chữ cái viết hoa (A - Z), chữ cái viết thường (a - z), chữ số (0 - 9) và các ký tự đặc biệt khác trên bàn phím máy tính và dấu cách.

b) Mật khẩu không chứa tên tài khoản.

c) Mật khẩu phải được thay đổi tối thiểu 06 tháng một lần.

Chương III

ĐẢM BẢO AN NINH MẠNG

Điều 12. Các hoạt động bảo vệ an ninh mạng

Việc triển khai các hoạt động bảo vệ an ninh mạng do đơn vị quản lý hệ thống thông tin chịu trách nhiệm, bao gồm:

1. Xác định rõ hệ thống thông tin quan trọng cần ưu tiên bảo đảm an ninh mạng.

2. Xây dựng quy định, 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.

3. Xây dựng 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.

4. Đảm bảo 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.

5. 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.

6. Quy định chế tài xử lý những vi phạm quy định về đảm bảo an ninh mạng.

7. Quy định về đảm bảo trang bị các phần mềm, công cụ... thực hiện việc giám sát, cảnh báo, ngăn chặn các cuộc tấn công; bóc gỡ thành phần mã độc bị cài đặt khai thác.

Điều 13. Xác định rõ hệ thống thông tin quan trọng cần ưu tiên bảo đảm an ninh mạng

1. Đơn vị quản lý thống thông tin, đơn vị vận hành hệ thống thông tin, đơn vị chuyên trách an toàn an ninh mạng có trách nhiệm bảo đảm an ninh mạng cho hệ thống thông tin quan trọng về an ninh quốc gia theo quy định từ Điều 12 đến Điều 15 của Luật An ninh mạng, Điều 7 đến Điều 17 của Nghị định số 53/2022/NĐ-CP.

2. Đơn vị không thuộc phạm vi khoản 1 Điều này có trách nhiệm:

a) Bảo đảm an toàn an ninh mạng cho máy tính của người sử dụng thuộc đơn vị: sử dụng hệ điều hành được hỗ trợ bản vá lỗ hổng bảo mật; chỉ cài đặt tiện ích thiết yếu được cung cấp kèm theo hệ điều hành và các phần mềm phục vụ công việc, phần mềm có bản quyền hoặc được các cơ quan chức năng đánh giá, xác nhận an toàn; cài đặt phần mềm phòng, diệt mã độc và cập nhật thường xuyên mẫu nhận diện mã độc.

b) Bảo đảm an toàn an ninh mạng cho thiết bị mạng, thiết bị an ninh mạng sử dụng tại đơn vị: không sử dụng thiết bị không còn được hỗ trợ khắc phục lỗ hổng bảo mật; thực hiện khắc phục lỗ hổng bảo mật ngay khi nhận được cảnh báo, hướng dẫn từ cơ quan chức năng; thay đổi mật khẩu mặc định và giữ bí mật mật khẩu quản trị thiết bị.

Điều 14. Xây dựng Quy định quản lý, nghiệp vụ, kỹ thuật trong vận hành hệ thống thông tin

Đơn vị quản lý hệ thống thông tin có trách nhiệm triển khai hoạt động bảo vệ an ninh mạng thuộc quyền quản lý. Triển khai xây dựng các quy định dựa trên một số quy định tại Chương II của quy chế này.

Điều 15. Giám sát an toàn, an ninh thông tin mạng

1. Đơn vị quản lý hệ thống thông tin có nhiệm vụ, trách nhiệm:

a) Chỉ đạo việc giám sát an ninh thông tin mạng đối với các hệ thống thông tin thuộc phạm vi quản lý, phối hợp với Cục Công nghệ thông tin và các đơn vị chức năng của Bộ Thông tin và Truyền thông giám sát theo quy định.

b) Các hệ thống thông tin bắt buộc phải có chức năng ghi và lưu trữ nhật ký về hoạt động của hệ thống và người sử dụng hệ thống thông tin. Thực hiện việc bảo vệ các chức năng ghi nhật ký và thông tin nhật ký, chống giả mạo, sửa đổi, phá hủy và truy cập trái phép.

c) Đơn vị chủ quản hệ thống thông tin của các đơn vị thuộc Bộ cử 01 lãnh đạo đơn vị và 01 cán bộ làm đầu mối giám sát an toàn, an ninh thông tin để tiếp nhận cảnh báo, cung cấp, trao đổi, chia sẻ thông tin với Cục Công nghệ thông tin trong các hoạt động giám sát an toàn, an ninh thông tin tại đơn vị và tại Bộ Giáo dục và Đào tạo.

d) Tuân thủ các quy định tại Điều 11, Quyết định 3710/QĐ-BGDĐT ngày 16/11/2022 Ban hành Quy chế đảm bảo An toàn thông tin mạng của Bộ Giáo dục và Đào tạo.

2. Đơn vị quản lý hệ thống thông tin quan trọng về an ninh quốc gia phối hợp với Cục An ninh mạng và phòng chống tội phạm công nghệ cao của Bộ Công an triển khai giám sát an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia theo quy định tại khoản 3 Điều 15 Nghị định số 53/2022/NĐ-CP.

Điều 16. Kiểm tra, đánh giá an toàn, an ninh thông tin

1. Đơn vị chủ quản hệ thống thông tin:

a) Có thẩm quyền yêu cầu kiểm tra, đánh giá an toàn, an ninh thông tin đối với các hệ thống thông tin thuộc thẩm quyền quản lý, có thẩm quyền giao nhiệm vụ hoặc được lựa chọn thuê dịch vụ để thực hiện việc kiểm tra, đánh giá. Đối tượng kiểm tra, đánh giá là Đơn vị quản lý, sử dụng hệ thống thông tin hoặc đơn vị vận hành hệ thống thông tin và các hệ thống thông tin có liên quan.

b) Hệ thống thông tin quan trọng về an ninh quốc gia thực hiện trình tự, thủ tục đánh giá, kiểm tra theo quy định tại Điều 14, Điều 16 Nghị định số 53/2022/NĐ-CP và theo hướng dẫn của Bộ Công an. Tổ chức, doanh nghiệp cung cấp dịch vụ kiểm tra, đánh giá an toàn, an ninh mạng phải độc lập với tổ chức, doanh nghiệp cung cấp dịch vụ giám sát an toàn, an ninh mạng cho đơn vị.

2. Cục Công nghệ thông tin:

a) Có thẩm quyền yêu cầu kiểm tra, đánh giá đối với các hệ thống thông tin do các đơn vị phê duyệt hồ sơ đề xuất cấp độ.

b) 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 Giáo dục và Đào tạo theo quy định tại Điều 12 Thông tư số 12/2022/TT-BTTTT.

c) Thực hiện việc đánh giá hiệu quả 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 17. Ứng cứu sự cố an toàn, an ninh thông tin

Đơn vị quản lý hệ thống thông tin:

1. Tuân thủ quy định tại Điều 12, Quyết định 3710/QĐ-BGDĐT ngày 16/11/2022 Ban hành Quy chế đảm bảo An toàn thông tin mạng của Bộ Giáo dục và Đào tạo.

2. Đối với hệ thống thông tin quan trọng về an ninh quốc gia, áp dụng trình tự, thủ tục ứng phó, khắc phục sự cố an ninh mạng theo quy định tại Điều 17 của Nghị định số 53/2022/NĐ-CP.

Điều 18. Phổ biến, tuyên truyền, đào tạo, bồi dưỡng về an ninh mạng

1. Thủ trưởng các đơn vị thuộc Bộ tổ chức quán triệt, tuyên truyền, phổ biến, nâng cao nhận thức, trách nhiệm về an toàn an ninh mạng cho cán bộ, công chức, viên chức, người lao động thuộc đơn vị.

2. Cục Công nghệ thông tin phối hợp các đơn vị liên quan tổ chức tập huấn, bồi dưỡng theo các chương trình đào tạo ngắn hạn nâng cao kiến thức, kỹ năng về an toàn an ninh mạng cho công chức, viên chức các đơn vị thuộc Bộ.

Chương IV

TỔ CHỨC THỰC HIỆN

Điều 19. Cục Công nghệ thông tin

1. Thực hiện các trách nhiệm được giao tại Quy chế này.

2. Hướng dẫn, giám sát, đôn đốc triển khai Quy chế này và các quy định khác có liên quan.

3. Thực hiện trách nhiệm của đơn vị chuyên trách về an toàn thông tin theo quy định tại Quy chế này và các nhiệm vụ do Bộ Giáo dục và Đào tạo phân công.

4. Phối hợp chặt chẽ với đơn vị vận hành hệ thống thông tin trong việc bảo đảm an toàn thông tin trong tất cả các công đoạn liên quan đến hệ thống thông tin.

5. Chủ trì/phối hợp với các đơn vị trong việc hướng dẫn, hỗ trợ các cơ quan, đơn vị về công tác bảo đảm an toàn thông tin và an ninh mạng.

6. Chủ trì/phối hợp với Đơn vị trong việc xây dựng kế hoạch, báo cáo về an toàn thông tin mạng và an ninh mạng của Bộ Giáo dục và Đào tạo.

7. Bảo đảm an toàn, an ninh thông tin cho các hệ thống thông tin, cơ sở dữ liệu dùng chung của Bộ.

8. Tổ chức tập huấn, bồi dưỡng theo các chương trình đào tạo ngắn hạn nâng cao kiến thức, kỹ năng về an toàn an ninh mạng cho công chức, viên chức các đơn vị thuộc Bộ Giáo dục và Đào tạo.

Điều 20. Các đơn vị thuộc Bộ

1. Thực hiện các trách nhiệm được giao tại Quy chế này.

2. Thực hiện việc quản lý trang thiết bị công nghệ thông tin và cán bộ, công chức, viên chức, người lao động theo Điều 6, Điều 8 và Điều 11 của Quy chế này.

3. Phối hợp với Cục Công nghệ thông tin bảo đảm an toàn, an ninh thông tin cho các hệ thống thông tin, cơ sở dữ liệu dùng chung của Bộ và các hệ thống thông tin do đơn vị quản lý, vận hành hệ thống thông tin.

Điều 21. Đơn vị quản lý, vận hành hệ thống thông tin

1. Thực hiện trách nhiệm của đơn vị quản lý, vận hành hệ thống thông tin theo quy định tại Quy chế này.

2. Thực hiện các báo cáo theo quy định, gửi Cục Công nghệ thông tin tổng hợp, báo cáo Bộ.

3. Xây dựng, triển khai Quy chế/nội quy bảo đảm an toàn, an ninh thông tin tại đơn vị bảo đảm phù hợp với Quyết định 3710/QĐ-BGDĐT ngày 16/11/2022 của Bộ Giáo dục và Đào tạo và với Quy chế này.

Điều 22. Công chức, viên chức và người lao động

Công chức, viên chức và người lao động của các đơn vị thuộc Bộ có trách nhiệm: tuân thủ Quy chế; thông báo các vấn đề bất thường liên quan tới an toàn thông tin cho Thủ trưởng đơn vị và chịu trách nhiệm trước pháp luật, trước lãnh đạo đơn vị về các vi phạm, thất thoát dữ liệu mật do không tuân thủ Quy chế.

Điều 23. Kinh phí thực hiện

1. Kinh phí bảo đảm an toàn thông tin mạng và an ninh mạng được lấy từ nguồn ngân sách nhà nước dự toán hàng năm của Bộ Giáo dục và Đào tạo.

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 thông tin mạng và an ninh mạng gửi Vụ Kế hoạch - Tài chính thẩm định, trình lãnh đạo Bộ phê duyệt.

Điều 24. Công tác kiểm tra

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

2. Giao Cục Công nghệ thông tin kiểm tra và báo cáo Lãnh đạo Bộ việc thực hiện Quy chế này tại các đơn vị thuộc Bộ Giáo dục và Đào tạo.

Điều 25. Chế độ báo cáo

1. Các đơn vị có liên quan thuộc Bộ có trách nhiệm lập báo cáo định kỳ, đột xuất theo yêu cầu và hướng dẫn của Cục Công nghệ thông tin.

2. Cục Công nghệ thông tin chịu trách nhiệm tổng hợp báo cáo của các đơn vị, trình Lãnh đạo Bộ Giáo dục và Đào tạo phê duyệt, gửi các cơ quan quản lý nhà nước về an toàn thông tin, an ninh mạng theo quy định.

Điều 26. Khen thưởng, kỷ luật

1. Kết quả thực hiện Quy chế này là một trong những tiêu chí có thể sử dụng để đánh giá kết quả thực hiện hàng năm của cá nhân, đơn vị.

2. Đơn vị, cá nhân vi phạm Quy chế này và các quy định khác của pháp luật về bảo đảm an toàn thông tin mạng và an ninh mạng, tùy theo tính chất, mức độ vi phạm sẽ bị xử lý kỷ luật hoặc các

hình thức xử lý khác theo quy định của pháp luật; nếu vi phạm gây thiệt hại đến tài sản, thiết bị, thông tin, dữ liệu thì chịu trách nhiệm bồi thường theo quy định pháp luật hiện hành.

Điều 27. Trách nhiệm thi hành

1. Thủ trưởng các đơn vị thuộc Bộ có trách nhiệm phổ biến, quán triệt đến toàn thể cán bộ công chức, viên chức và người lao động trong đơn vị thực hiện các quy định của Quy chế này.

2 Trong quá trình thực hiện, nếu có những vấn đề khó khăn, vướng mắc, các đơn vị phản ánh về Cục Công nghệ thông tin để tổng hợp, trình Bộ trưởng xem xét, sửa đổi, bổ sung Quy chế./.