BỘ GIÁO DỤC VÀ ĐÀO TẠO

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

QUY CHẾ
ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG CỦA BỘ GIÁO DỤC VÀ ĐÀO TẠO

(Kèm theo Quyết định số 3710 /QĐ-BGDĐT ngày 16 /11/2022 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. Quy chế này quy định về đảm bảo An toàn thông tin mạng trong các hoạt động ứng dụng công nghệ thông tin của Bộ Giáo dục và Đào tạo (sau đây gọi tắt là Bộ).

2. Quy chế này áp dụng đối với:

a) Các cơ quan, đơn vị thuộc Bộ (sau đây gọi tắt là đơn vị) và công chức, viên chức, người lao động của Bộ (sau đây gọi là cá nhân).

b) Cơ quan, tổ chức, cá nhân có sử dụng hoặc kết nối truy cập vào hệ thống mạng của Bộ.

Điều 2. Giải thích từ ngữ

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

1. Hệ thống mạng: bao gồm dịch vụ kết nối Internet; mạng nội bộ; mạng truyền số liệu chuyên dùng.

2. *Mạng nội bộ (LAN):* là tập hợp các trang thiết bị công nghệ thông tin được kết nối với nhau thông qua các bộ chuyển mạch, bộ định tuyến, bộ điểm truy cập và các máy chủ, thiết bị quản lý mạng, phần mềm quản lý mạng, thiết bị an toàn hệ thống mạng trong phạm vi quản lý của Bộ. Mạng nội bộ bao gồm mạng nội bộ có dây và mạng nội bộ không dây (Wifi).

3. Phòng máy chủ, bao gồm: hệ thống máy chủ, thiết bị chuyển mạch, thiết bị định tuyến, thiết bị lưu trữ, thiết bị đảm bảo 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 đặt tại phòng máy chủ.

4. *Mạng truyền số liệu chuyên dùng*: là mạng của các cơ quan Đảng, Nhà nước, là hệ thống thông tin quan trọng quốc gia, được sử dụng riêng trong hoạt động truyền số liệu và ứng dụng công nghệ thông tin của các cơ quan Đảng, Nhà

nước, do Bộ Thông tin và Truyền thông quản lý.

5. 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) của cá nhân.

6. Đơn vị vận hành hệ thống thông tin: là đơn vị chủ trì việc quản lý và vận hành kỹ thuật hệ thống thông tin.

Điều 3. Phạm vi đảm bảo an toàn thông tin

1. Hệ thống phòng máy chủ.

2. Hệ thống mạng.

3. Hệ thống thông tin quản lý, gồm: các phần mềm nghiệp vụ và cơ sở dữ liệu phục vụ công tác quản lý, điều hành hoạt động của Bộ.

4. Trang thiết bị công nghệ thông tin cá nhân.

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

1. Đảm bảo an toàn thông tin mạng là yêu cầu bắt buộc, thường xuyên, liên tục, có tính xuyên suốt quá trình, đồng bộ từ khi thiết kế, xây dựng, vận hành, nâng cấp và hủy bỏ (dừng hoạt động) hệ thống thông tin. Đảm bảo an toàn thông tin mạng phải tuân thủ các nguyên tắc chung, được quy định tại Điều 4 Luật An toàn thông tin mạng và Điều 4 Nghị định số 85/2016/NĐ-CP ngày 01/07/ 2016 của Chính phủ.

2. Đơn vị vận hành hệ thống thông tin có trách nhiệm đảm bảo an toàn thông tin 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 mạng đối với các hệ thống thông tin do đơn vị mình quản lý.

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

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

Điều 5. Các hành vi bị nghiêm cấm

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

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

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

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

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

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

7. Các hành vi bị nghiêm cấm quy định tại Điều 8 Luật An ninh mạng.

Chương II
QUY ĐỊNH ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 6. Đảm bảo an toàn thông tin Hệ thống Phòng máy chủ

1. Cục Công nghệ thông tin là đơn vị quản lý, vận hành hệ thống phòng máy chủ của Bộ.

2. Đơn vị quản lý vận hành phòng máy chủ có trách nhiệm xây dựng nội quy quản lý, vận hành đảm bảo các quy định an toàn thông tin.

3. Phòng máy chủ là khu vực hạn chế tiếp cận; chỉ những cá nhân có quyền, nhiệm vụ theo quy định mới được phép vào phòng máy chủ.

Điều 7. Đảm bảo an toàn thông tin Hệ thống mạng

1. Mạng nội bộ và dịch vụ Internet

a) Quản lý mạng nội bộ

- Cục Công nghệ thông tin là đơn vị quản lý, vận hành mạng nội bộ và dịch vụ Internet của Bộ.

- Cục Công nghệ thông tin có trách nhiệm ban hành nội quy nội bộ về quản lý, vận hành kỹ thuật mạng nội bộ của Bộ và tổ chức thực hiện; triển khai biện pháp kỹ thuật giám sát kết nối mạng Internet của thiết bị đầu cuối, phát hiện và ngăn chặn các hành vi xâm nhập từ mạng Internet.

b) Sử dụng mạng nội bộ và Internet

- Bộ Giáo dục và Đào tạo cung cấp 2 tên định danh mạng nội bộ không dây có kết nối Internet gồm: MOET và MOET_GUEST. Mạng MOET cung cấp cho công chức, viên chức và người lao động của Bộ với chất lượng truy cập cao. Mạng MOET_GUEST cung cấp dịch vụ truy cập Internet cho khách đến công tác ở cơ quan Bộ.

- Để kết nối và sử dụng dịch vụ mạng không dây MOET (đối với các thiết bị chưa kết nối được với mạng MOET), đơn vị/cá nhân gửi thông tin địa chỉ vật lý của thiết bị (dạng 0A:1B:2C:FF:FF:FF) cần kết nối tới địa chỉ thư điện tử của Cục Công nghệ thông tin cuccntt@moet.gov.vn để được hỗ trợ và cấp quyền truy cập.

- Các đơn vị và cá nhân có trách nhiệm quản lý và bảo quản các trang thiết bị công nghệ thông tin và tài nguyên mạng nội bộ lắp đặt tại phòng làm việc của đơn vị.

- Khi phát hiện nguy cơ mất an toàn thông tin (cảnh báo từ phần mềm phòng chống mã độc, máy tính hoạt động chậm bất thường, mất dữ liệu), đơn vị và cá nhân phải tắt thiết bị công nghệ thông tin, kịp thời thông báo với Cục Công nghệ thông tin để được hỗ trợ xử lý.

2. Mạng truyền số liệu chuyên dùng

a) Cục Công nghệ thông tin là đơn vị quản lý, vận hành mạng truyền số liệu chuyên dùng của cơ quan Bộ.

b) Cục Công nghệ thông tin ban hành nội quy nội bộ về quản lý, vận hành, đảm bảo theo các quy định của Bộ Thông tin và Truyền thông và tổ chức thực hiện kết nối các dịch vụ của Bộ vào mạng truyền số liệu chuyên dùng.

Điều 8. Đảm bảo an toàn thông tin đối với các Hệ thống thông tin quản lý và cơ sở dữ liệu của Bộ

1. Đảm bảo an toàn thông tin trong xây dựng, nâng cấp hệ thống thông tin và cơ sở dữ liệu

a) Khi xây dựng mới hoặc nâng cấp hệ thống thông tin, đơn vị quản lý hệ thống thông tin có trách nhiệm xây dựng phương án bảo đảm an toàn cho các hệ thống thông tin; rà soát cấp độ 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.

b) Quá trình tổ chức xây dựng, nâng cấp hệ thống thông tin phải tuân thủ phương án bảo đảm an toàn thông tin đã đề xuất và theo các quy định của quản lý dự án công nghệ thông tin của Chính phủ.

2. Đảm bảo an toàn thông tin khi đưa vào khai thác sử dụng hệ thống thông tin và cơ sở dữ liệu

a) Đảm bảo an toàn thông tin trong quản lý hệ thống thông tin

- Các đơn vị vận hành hệ thống thông tin chịu trách nhiệm đảm bảo an toàn thông tin cho các hệ thống thông tin theo quy định tại các Điều 22, 23 và 24 của Luật An toàn thông tin mạng năm 2015.

- Cục Công nghệ thông tin là bộ phận chuyên trách về An toàn thông tin của Bộ; chịu trách nhiệm đảm bảo an toàn thông tin cho các hệ thống thông tin dùng chung của Bộ và thẩm định phương án bảo đảm an toàn cho các hệ thống thông tin trong phạm vi quản lý của Bộ.

- Đơn vị chủ trì xây dựng hệ thống thông tin khi bàn giao hệ thống thông tin về Cục Công nghệ thông tin 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.

b) Đảm bảo an toàn thông tin trong vận hành hệ thống thông tin

- Ngoài việc thực hiện các quy định tại văn bản này, Đơn vị vận hành hệ thống thông tin phải thực hiện các quy định về đảm bảo an toàn thông tin theo Điều 22, Nghị định số 85/2016/NĐ-CP ngày 01/07/ 2016 của Chính phủ.

- 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 thông tin nhật ký hệ thống thông tin để phục vụ quản lý và kiểm soát thông tin.

c) Đảm bảo an toàn thông tin 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. Đặt mật khẩu 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 01 lần / 6 tháng. 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.

- Cá nhân thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ hưu hoặc 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.

Điều 9. Đảm bảo an toàn thông tin trang thiết bị công nghệ thông tin cá nhân

1. Cá nhân chịu trách nhiệm về đảm bảo an toàn thông tin thiết bị do mình quản lý và sử dụng.

2. Các thiết bị công nghệ thông tin cá nhân phải được cài đặt và cập nhật thường xuyên phần mềm phòng chống mã độc; thực hiện kiểm tra, rà quét bằng phần mềm phòng chống mã độc 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.

3. Cá nhân chịu trách nhiệm và có biện pháp đảm bảo an toàn thông tin, tránh bị lộ lọt dữ liệu khi thực hiện bảo hành, bảo dưỡng, sửa chữa hoặc bảo trì thiết bị do mình quản lý.

4. Khi ngừng sử dụng thiết bị công nghệ thông tin cá nhân, cá nhân phải thực hiện tiêu hủy dữ liệu theo quy định.

Điều 10. Xác định cấp độ và phương án đảm bảo an toàn hệ thống thông tin

1. Các hệ thống thông tin phải thực hiện đảm bảo an toàn thông tin cấp độ (quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/07/ 2016 của Chính phủ).

2. Xác định cấp độ cho các hệ thống thông tin: Đơn vị vận hành hệ thống thông tin có trách nhiệm lập hồ sơ đề xuất cấp độ an toàn thông tin; Cục Công nghệ thông tin tổ chức thẩm định, phê duyệt hồ sơ đề xuất cấp độ theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/07/ 2016 của Chính phủ.

3. Phương án đảm bảo an toàn hệ thống thông tin theo cấp độ

a) Cục Công nghệ thông tin là đơn vị chuyên trách về an toàn thông tin của Bộ; chịu trách nhiệm giám sát, kiểm tra, đánh giá việc triển khai các phương án đảm bảo an toàn thông tin đã được phê duyệt.

b) Phương án đảm bảo 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 ngày 12/8/2022 của Bộ Thông tin và Truyền thông, phù hợp với tiêu chuẩn TCVN 11930:2017 và quy định về an toàn thông tin mạng của Bộ.

c) Đơn vị vận hành hệ thống thông tin có trách nhiệm tổ chức triển khai phương án đảm bảo an toàn hệ thống thông tin sau khi được phê duyệt.

Điều 11. Giám sát an toàn hệ thống thông tin

1. Các hệ thông tin phải được thực hiện giám sát an toàn thông tin.

2. Đơn vị vận hành hệ thống có trách nhiệm phối hợp với Cục Công nghệ thông tin (đơn vị chuyên trách an toàn thông tin của Bộ) tổ chức thực hiện việc giám sát hệ thống thông tin theo Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 về quy định hoạt động giám sát an toàn hệ thống thông tin của Bộ Thông tin và Truyền thông.

Điều 12. Ứng cứu sự cố an toàn hệ thống thông tin

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

a) Cục Công nghệ thông tin là đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng của Bộ. Đơn vị 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 ngày 16/03/2017 của Thủ tướng Chính phủ.

b) Cục Công nghệ thông tin theo kế hoạch hằng năm, có trách nhiệm trình lãnh đạo Bộ kiện toàn Đội ứng cứu an toàn thông tin mạng của Bộ và tổ chức ứng cứu sự cố trong phạm vi của Bộ.

2. Kế hoạch ứng phó sự cố đảm bảo an toàn thông tin mạng: Trước ngày 31 tháng 10 hàng năm, Cục Công nghệ thông tin có trách nhiệm xây dựng và trình lãnh đạo bộ ban hành Kế hoạch ứng cứu sự cố bảo đảm an toàn thông tin mạng theo đề cương tại Phụ lục II, Quyết định số 05/2017/QĐ-TTg ngày 16/03/2017 của Thủ tướng Chính phủ.

3. Quy trình ứng cứu sự cố An toàn thông tin mạng Được thực hiện theo Quyết định số 05/2017/QĐ-TTg ngày 16/03/2017 của Thủ tướng Chính phủ và Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông.

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

a) Cục Công nghệ thông tin chủ trì, phối hợp với các đơn vị thuộc Bộ 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.

b) Đơn vị vận hành hệ thống thông tin tổ chức tham gia diễn tập ứng cứu sự cố theo kế hoạch ứng phó sự cố đã được lãnh đạo Bộ phê duyệt.

Chương III
TỔ CHỨC THỰC HIỆN

Điều 13. Trách nhiệm của các đơn vị thuộc Bộ

1. Tổ chức phổ biến, chỉ đạo việc tuân thủ các quy định tại Quy chế này và các văn bản quy định có liên quan khác của Nhà nước đối với các cá nhân thuộc đơn vị mình về an toàn thông tin mạng.

2. Thường xuyên kiểm tra, đôn đốc việc triển khai an toàn thông tin mạng trong công việc của cá nhân do mình quản lý.

3. Thực hiện các báo cáo theo yêu cầu gửi Cục Công nghệ thông tin, để tổng hợp, báo cáo Lãnh đạo Bộ.

Điều 14. Trách nhiệm của cá nhân

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

2. Tham gia đầy đủ các lớp đào tạo ngắn hạn, tuyên truyền, phổ biến nâng cao nhận thức, diễn tập an toàn thông tin và ứng cứu sự cố để bảo đảm an toàn thông tin mạng theo kế hoạch.

3. Chịu trách nhiệm trước lãnh đạo đơn vị và lãnh đạo Bộ về các vi phạm làm mất an toàn thông tin mạng do không tuân thủ Quy chế này.

Điều 15. Trách nhiệm của Cục Công nghệ thông tin

1. Chủ trì tổ chức theo dõi, đôn đốc, kiểm tra và đánh giá việc thực hiện Quy chế này.

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

3. Hỗ trợ các đơn vị, cá nhân về công tác bảo đảm an toàn thông tin mạng.

Điều 16. Kinh phí thực hiện

1. Kinh phí đảm bảo ATTT mạng thực hiện lồng ghép, tích hợp với các chương trình, đề án, nhiệm vụ công nghệ thông tin từ nguồn ngân sách nhà nước và các nguồn kinh phí hợp pháp khác.

2. Các đơn vị vận hành hệ thống thông tin có trách nhiệm xây dựng kế hoạch, đề xuất dự toán kinh phí cho các hoạt động đảm bảo an toàn thông tin mạng, gửi Cục Công nghệ thông tin thẩm định về chuyên môn và gửi Vụ Kế hoạch - Tài chính thẩm định và trình lãnh đạo Bộ phê duyệt.

Điều 17. Trách nhiệm thi hành

1. Thủ trưởng các đơn vị thuộc Bộ có trách nhiệm phổ biến, quán triệt đến

toàn bộ công chức, viên chức và người lao động trong đơn vị thực hiện các quy định của Quy chế này; thường xuyên kiểm tra việc thực hiện Quy chế này tại đơn vị; chịu trách nhiệm trước pháp luật và Lãnh đạo Bộ về các vi phạm, thất thoát thông tin, dữ liệu thuộc phạm vi quản lý của đơn vị, do không tổ chức, chỉ đạo và kiểm tra cán bộ của đơn vị thực hiện đúng Quy chế.

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