

Số: 51 /QĐ-TCGDNN

Hà Nội, ngày 13 tháng 3 năm 2024

QUYẾT ĐỊNH

Ban hành Quy chế đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của Tổng cục Giáo dục nghề nghiệp

TỔNG CỤC TRƯỞNG TỔNG CỤC GIÁO DỤC NGHỀ NGHIỆP

Căn cứ Luật Công nghệ thông tin năm 2006;

Căn cứ Luật An toàn thông tin mạng năm 2015;

Căn cứ Luật An ninh mạng năm 2018;

Căn cứ Luật Bảo vệ bí mật nhà nước năm 2018;

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan Nhà nước;

Căn cứ Nghị định số 72/2013/NĐ-CP ngày 15/7/2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng;

Căn cứ 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;

Căn cứ Nghị định số 142/2016/NĐ-CP ngày 14/10/2016 của Chính phủ về ngăn chặn xung đột thông tin trên mạng;

Căn cứ Thông tư số 27/2017/TT-BTTTT ngày 20/10/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về việc 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 Nghị định số 26/2020/NĐ-CP ngày 28/02/2020 của Chính phủ quy định chi tiết một số điều của luật bảo vệ bí mật nhà nước;

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

Căn cứ Quyết định số 29/2017/QĐ-TTg ngày 03/07/2017 của Thủ tướng Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của nhiệm vụ Tổng cục Giáo dục nghề nghiệp thuộc Bộ Lao động - Thương binh và Xã hội;

Căn cứ Quyết định 234/QĐ-BLĐTBXH ngày 06/3/2024 của Bộ trưởng Bộ Lao động - Thương binh và Xã hội ban hành Quy chế bảo đảm an toàn thông tin,

an ninh mạng trong hoạt động ứng dụng công nghệ thông tin và chuyển đổi số của Bộ Lao động - Thương binh và Xã hội;

Theo đề nghị của Chánh Văn phòng Tổng cục Giáo dục nghề nghiệp,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này “Quy chế đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của Tổng cục Giáo dục nghề nghiệp”.

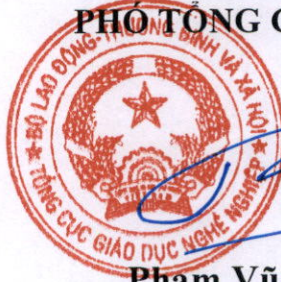
Điều 2. Quyết định này có hiệu lực kể từ ngày ký.

Điều 3. Chánh Văn phòng, thủ trưởng các Vụ, đơn vị, cá nhân thuộc Tổng cục Giáo dục nghề nghiệp thực hiện Quyết định này. *uuy*

Nơi nhận:

- Như Điều 3;
- Tổng cục trưởng (để b/c);
- Các Phó Tổng cục trưởng;
- Trung tâm CNTT Bộ;
- Lưu: VT, TT-TT.

**KT. TỔNG CỤC TRƯỞNG
PHÓ TỔNG CỤC TRƯỞNG**



Phạm Vũ Quốc Bình

QUY CHẾ

**đảm bảo an toàn thông tin mạng trong hoạt động
ứng dụng công nghệ thông tin của Tổng cục Giáo dục nghề nghiệp**
(Ban hành kèm theo Quyết định số 51 /QĐ-TCGDNN ngày 13 tháng 3 năm 2024
của Tổng cục trưởng Tổng cục Giáo dục nghề nghiệp)

Chương I

QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định việc đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin, mạng máy tính của Tổng cục Giáo dục nghề nghiệp.

Điều 2. Đối tượng áp dụng

Quy chế này được áp dụng đối với các Vụ, đơn vị, công chức, viên chức và người lao động thuộc Tổng cục Giáo dục nghề nghiệp trong việc quản lý, khai thác, sử dụng và đảm bảo an toàn, an ninh thông tin của Tổng cục phục vụ công tác chuyên môn.

Điều 3. Giải thích từ ngữ

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

1. An toàn thông tin mạng là công tác 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. Hệ thống thông tin là tập hợp 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 của một cơ quan, tổ chức.

3. Sự cố an toàn thông tin mạng là việc thông tin, hệ thống thông tin bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.

4. Phần mềm độc hại là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

5. Cán bộ chuyên trách là cán bộ, công chức, viên chức, người lao động được tuyển dụng phụ trách an toàn thông tin/công nghệ thông tin tại các cơ quan, đơn vị.

Điều 4. Nguyên tắc bảo đảm an toàn thông tin

1. Cơ quan, tổ chức, cá nhân có trách nhiệm bảo đảm an toàn thông tin mạng. Hoạt động an toàn thông tin mạng của cơ quan, tổ chức, cá nhân phải đúng quy định của pháp luật, bảo đảm quốc phòng, an ninh quốc gia, bí mật nhà nước, giữ vững ổn định chính trị, trật tự, an toàn xã hội và thúc đẩy phát triển kinh tế - xã hội.

2. Tổ chức, cá nhân không được xâm phạm an toàn thông tin mạng của tổ chức, cá nhân khác.

3. Việc xử lý sự cố an toàn thông tin mạng phải bảo đảm quyền và lợi ích hợp pháp của tổ chức, cá nhân, không xâm phạm đến đời sống riêng tư, bí mật cá nhân, bí mật gia đình của cá nhân, thông tin riêng của tổ chức.

4. Hoạt động an toàn thông tin mạng phải được thực hiện thường xuyên, liên tục, kịp thời và hiệu quả.

Chương II

QUY ĐỊNH ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 5. Bảo vệ bí mật nhà nước trong hoạt động ứng dụng công nghệ thông tin

1. Quy định về soạn thảo, in ấn, phát hành và sao chụp tài liệu mật

a) Việc soạn thảo, in ấn, phát hành và sao chụp tài liệu mật phải đảm bảo theo quy định tại Điều 3 Nghị định số 26/2020/NĐ-CP ngày 28/02/2020 của Chính phủ quy định chi tiết một số điều của luật bảo vệ bí mật nhà nước.

b) Không được sử dụng máy tính nối mạng Internet để soạn thảo văn bản; chuyển giao, lưu trữ thông tin có nội dung thuộc bí mật nhà nước; cung cấp tin, tài liệu và đưa thông tin bí mật nhà nước trên Cổng/Trang thông tin điện tử;

c) Không được in, sao chụp tài liệu bí mật nhà nước trên các thiết bị kết nối mạng Internet;

d) Văn phòng bố trí 01 máy vi tính riêng, không kết nối mạng nội bộ và mạng Internet dùng để quản lý, soạn thảo các tài liệu mật của nhà nước theo quy định. Người soạn thảo văn bản mật của các Vụ, đơn vị thuộc Tổng cục soạn thảo trên máy vi tính này hoặc máy tính của Vụ, đơn vị được bố trí riêng, không kết nối mạng nội bộ và mạng Internet.

2. Khi sửa chữa, khắc phục các sự cố của máy tính dùng soạn thảo văn bản mật, các phòng, đơn vị phải báo cáo cho người có thẩm quyền. Không được cho phép các tổ chức, cá nhân không có trách nhiệm trực tiếp sửa chữa, xử lý, khắc phục sự cố.

3. Trước khi thanh lý các máy tính trong đơn vị cán bộ chuyên trách công nghệ thông tin phải dùng các biện pháp kỹ thuật xóa bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính.

Điều 6. Bảo đảm an toàn hạ tầng mạng

1. Thiết bị công nghệ thông tin được trang bị tại các Vụ, đơn vị thuộc Tổng cục là tài sản của Nhà nước, được quản lý, sử dụng theo quy định của Nhà nước. Các Vụ, đơn vị, công chức, viên chức và người lao động có trách nhiệm quản lý trang thiết bị được giao.

2. Giao cho Văn phòng làm công tác quản trị mạng, quản lý kỹ thuật và duy trì hoạt động của hệ thống thông tin của Tổng cục; là đầu mối phối hợp với đơn vị phụ trách về công nghệ thông tin của Bộ và đơn vị quản trị của tòa nhà 37 Nguyễn Bình Khiêm, tòa nhà D25, ngõ 7 Tôn Thất Thuyết để kết nối mạng LAN, mạng

Internet, mạng dữ liệu chuyên dùng cho Tổng cục; kiểm tra hiện trạng, đề xuất sửa chữa hoặc mua mới các chủng loại thiết bị công nghệ thông tin, phần mềm, phần mềm chống mã độc, virus, phần mềm tường lửa,... phù hợp, an toàn, bảo mật theo quy định về quản lý, sử dụng tài sản cơ quan.

Điều 7. Bảo đảm an toàn dữ liệu

1. Quản lý tài khoản và chữ ký số

a) Khi được cấp tài khoản, chữ ký số người sử dụng thay đổi mật khẩu ngay sau khi đăng nhập lần đầu tiên và bảo vệ thông tin của tài khoản theo quy định. Mật mã đăng nhập, truy cập phải có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số hoặc ký tự đặc biệt như: !, @, #, \$, %, ...), định kỳ 6 tháng thay đổi mật khẩu nhằm tăng cường công tác bảo mật;

b) Chủ tài khoản, chữ ký số không chia sẻ, giao quyền tài khoản, chữ ký số và mật khẩu truy nhập cho người khác. Không sử dụng tài khoản của người khác (ví dụ tài khoản thư điện tử, chữ ký số, chứng thư số) để đăng nhập vào hệ thống thông tin, cơ sở dữ liệu;

c) Tài khoản thư điện tử, chữ ký số chuyên dùng (xxx@molisa.gov.vn và chữ ký số do Ban Cơ yếu Chính phủ cấp) để phục vụ cho các hoạt động mang tính công vụ, không sử dụng để giao dịch, đăng ký trên mạng xã hội, các trang thông tin điện tử công cộng khác;

d) Khi cá nhân thay đổi vị trí công tác, chuyển công tác, thôi việc, nghỉ hưu, ngay từ thời điểm Quyết định có hiệu lực, cơ quan, đơn vị quản lý cá nhân đó phải thông báo cho Văn phòng và Trung tâm Công nghệ Thông tin của Bộ để điều chỉnh, thu hồi, hủy bỏ tài khoản, chữ ký số, chứng thư số.

2. Trách nhiệm, quyền hạn người dùng khi truy cập, đăng nhập các hệ thống thông tin, đảm bảo mỗi người dùng khi sử dụng hệ thống thông tin phải được cấp và sử dụng tài khoản truy cập gắn với người dùng đó. Trường hợp sử dụng tài khoản dùng chung cho một nhóm người hay một đơn vị, phải có cơ chế xác định các cá nhân, đơn vị có trách nhiệm quản lý tài khoản. Người dùng chỉ được truy cập các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình và có trách nhiệm bảo mật tài khoản truy cập được cấp.

3. Khi thực hiện chia sẻ tài nguyên trên máy tính, các cá nhân, đơn vị phải sử dụng mật khẩu để bảo vệ thông tin, dữ liệu; không thực hiện chia sẻ toàn bộ ổ cứng; theo dõi, giám sát để kết thúc chia sẻ tài nguyên ngay khi hoàn thành. Các thông tin, tài liệu, dữ liệu nhạy cảm phải được mã hóa trước khi trao đổi, truyền nhận qua mạng máy tính.

4. Cá nhân sử dụng máy tính và thiết bị lưu trữ khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài cơ quan, đơn vị phải tháo rời bộ phận lưu trữ khỏi thiết bị và để lại cơ quan, đơn vị hoặc xóa dữ liệu lưu trữ trên thiết bị. Khi thanh lý thiết bị phải xóa dữ liệu lưu trữ bằng phần mềm hoặc thiết bị hủy dữ liệu chuyên dụng.

5. Thông tin, dữ liệu thuộc phạm vi bí mật Nhà nước phải được quản lý theo quy định hiện hành về bảo vệ bí mật Nhà nước.

Chương III

TRÁCH NHIỆM SỬ DỤNG VÀ TỔ CHỨC THỰC HIỆN

Điều 8. Bảo đảm an toàn máy tính cá nhân, bảo mật cơ sở dữ liệu và an ninh mạng

1. Văn phòng có trách nhiệm hỗ trợ cài đặt, quản lý các phần mềm hệ thống và phần mềm ứng dụng trong hệ thống mạng máy tính tại Tổng cục; nghiên cứu, đề xuất, nâng cấp công nghệ, phần mềm theo định hướng quản lý nhà nước của ngành và tuân theo quy định của Nhà nước.

2. Bảo mật số liệu: Công chức, viên chức, người lao động phải có trách nhiệm bảo mật số liệu nghiệp vụ trên máy tính.

3. Bảo mật truy cập: Các chương trình ứng dụng, phân chia sử dụng trên máy tính phải được đặt mật khẩu, mã khoá bảo mật.

4. Bảo mật hệ thống mạng và truyền tin: Mạng và đường truyền cần áp dụng các chế độ bảo mật cần thiết, chống xâm nhập bất hợp pháp. Văn phòng có trách nhiệm thường xuyên theo dõi, kiểm tra phát hiện kịp thời các hoạt động xâm nhập và có biện pháp xử lý kịp thời.

5. An toàn trong sử dụng: Khi không làm việc với máy vi tính trong thời gian dài, công chức, viên chức, người lao động thuộc Tổng cục phải tắt máy tính hoặc đặt chế độ bảo vệ để đảm bảo an toàn cho dữ liệu của cá nhân.

6. Phòng, chống virus: Công chức, viên chức, người lao động thuộc Tổng cục có trách nhiệm tuân thủ các biện pháp phòng và chống virus cho máy tính, đảm bảo an toàn dữ liệu thuộc cá nhân quản lý. Mọi dữ liệu từ các thiết bị lưu trữ bên ngoài đều phải được quét, diệt virus mỗi khi đưa vào máy. Những máy tính phát hiện có virus phải được tách khỏi mạng về mặt vật lý để tránh tình trạng lây nhiễm sang các máy tính khác. Không truy cập vào các liên kết (link) không rõ ràng; không nhấn (click), truy cập vào các link, tải về các tệp (file) tài liệu từ các địa chỉ thư điện tử (email) không nắm rõ thông tin, địa chỉ người gửi.

Điều 9. Trách nhiệm của công chức, viên chức, người lao động khi tham gia sử dụng và khai thác hệ thống thông tin tại Tổng cục Giáo dục nghề nghiệp

1. Nghiêm chỉnh thực hiện các nội quy, quy chế, quy trình nội bộ về bảo đảm an toàn thông tin, an ninh mạng của Tổng cục cũng như các quy định khác của pháp luật về nội dung này.

2. Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo kịp thời cho bộ phận chuyên trách công nghệ thông tin của Văn phòng để kịp thời ngăn chặn và xử lý.

3. Nâng cao ý thức cảnh giác và trách nhiệm về an toàn thông tin, an ninh mạng.

4. Không sử dụng mạng xã hội như: Google Plus+, MySpace, LinkedIn, Twitter, Facebook, Zalo,... blog cá nhân để đăng tải, phát tán, truyền tải lại những nội dung phản động, tuyên truyền, xuyên tạc; không được truy cập vào các liên kết

(link) không rõ ràng; không sử dụng địa chỉ thư điện tử công vụ vào mục đích cá nhân như: đăng ký tài khoản mạng xã hội, đăng ký mua sắm qua mạng...

5. Không sử dụng các hộp thư điện tử miễn phí Gmail, Yahoo,... trong hoạt động công vụ và tại máy tính có nối mạng ở đơn vị mình nhằm bảo đảm bảo mật, an toàn thông tin trên môi trường mạng.

6. Cá nhân sử dụng các thiết bị lưu trữ dữ liệu di động (máy tính xách tay, thiết bị số cầm tay, thẻ nhớ USB, ổ cứng di động, băng từ...) để lưu thông tin thuộc danh mục bí mật Nhà nước có trách nhiệm bảo vệ các thiết bị này và thông tin trên thiết bị, tránh làm mất, lộ thông tin và đảm bảo theo các quy định liên quan tại Nghị định số 26/2020/NĐ-CP ngày 28/02/2020 của Chính phủ quy định chi tiết một số điều của luật bảo vệ bí mật nhà nước.

7. Không được lợi dụng việc sử dụng mạng Internet nhằm mục đích: Chống lại nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội; kích động bạo lực, đòi truy, tệ nạn xã hội, mê tín dị đoan; phá hoại thuần phong mỹ tục của dân tộc; không được truy cập hoặc tải các trang website có nội dung đòi truy, phản động, các chương trình không rõ nguồn gốc, các thông tin quảng cáo trên mạng máy tính của cơ quan.

8. Không chơi các trò chơi trực tuyến (game online) hoặc các trò chơi khác trên mạng Internet trong giờ làm việc trên các máy tính của cơ quan trang bị để làm việc.

Điều 10. Tổ chức thực hiện

1. Căn cứ Quy chế, thủ trưởng các Vụ, đơn vị thuộc Tổng cục có trách nhiệm tổ chức triển khai thực hiện Quy chế trong phạm vi quản lý của mình.

2. Công chức, viên chức và người lao động tại các Vụ, đơn vị thuộc Tổng cục có trách nhiệm thực hiện nghiêm túc Quy chế này.

3. Giao Văn phòng có trách nhiệm theo dõi, đôn đốc, kiểm tra, đánh giá việc thực hiện Quy chế; đồng thời định kỳ báo cáo kết quả việc thực hiện quy chế cho Tổng cục trưởng theo quy định.

4. Vụ Kế hoạch - Tài chính tham mưu, trình Tổng cục trưởng bố trí kinh phí đảm bảo nguồn lực triển khai, đáp ứng yêu cầu về đảm bảo an toàn thông tin đối với những đề xuất sửa chữa hoặc mua mới các chủng loại thiết bị công nghệ thông tin, phần mềm, phần mềm chống mã độc, virus, phần mềm tường lửa....

5. Trong quá trình thực hiện, nếu có vấn đề phát sinh hoặc khó khăn, vướng mắc cần phản ánh kịp thời về Văn phòng để tổng hợp báo cáo Tổng cục trưởng xem xét quyết định điều chỉnh, bổ sung cho phù hợp./.

TỔNG CỤC GIÁO DỤC NGHỀ NGHIỆP