UBND TỈNH KHÁNH HÒA
TRƯỜNG CAO ĐẲNG Y TẾ

Số: 654 /QĐ-CĐYT

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

Khánh Hòa, ngày 07 tháng 11 năm 2018

QUYẾT ĐỊNH
Ban hành Quy định về việc đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin

HIỆU TRƯỞNG TRƯỜNG CAO ĐẲNG Y TẾ KHÁNH HÒA

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ quy định 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 tháng 7 năm 2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin điện tử trên Internet;

Căn cứ quyền hạn và trách nhiệm của Hiệu trưởng được quy định tại Điều lệ Trường Cao đẳng ban hành theo Thông tư số 46/2016/TT-BLĐTBXH ngày 28/12/2016 của Bộ Lao động – Thương binh và Xã hội;

Theo đề nghị của Trưởng Phòng Công nghệ thông tin,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy định về việc đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin.

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

Điều 3. Các ông, bà Trưởng Phòng : Công nghệ thông tin; các Phòng,Khoa, Bộ môn có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như điều 3;
- Đảng ủy Trường;
- Ban Giám hiệu;
- Lưu : VT, P.CNTT;

HIỆU TRƯỞNG

ỦY BAN NHÂN DÂN TỈNH KHÁNH HÒA
TRƯỜNG CAO ĐẲNG Y TẾ KHÁNH HÒA

Vũ Viết Sơn

TRƯỜNG CAO ĐẲNG Y TẾ
KHÁNH HÒA

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

QUY ĐỊNH
Về việc đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin

(Kèm theo Quyết định số 654 /QĐ-CĐYT ngày 07 tháng 11 năm 2018 của Hiệu trưởng Trường Cao đẳng Y tế Khánh Hòa)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi và đối tượng áp dụng

1. Phạm vi áp dụng:

Quy định này bao gồm các điều kiện tối thiểu phải tuân thủ nhằm đảm bảo an toàn thông tin trên môi trường máy tính, mạng máy tính. Thông tin được đảm bảo an toàn bao gồm tất cả các loại thông tin của Trường Cao đẳng Y tế Khánh Hòa và các Phòng, Khoa, Bộ môn trực thuộc, các thông tin do các cơ quan, tổ chức khác gửi đến Trường Cao đẳng Y tế Khánh Hòa.

2. Đối tượng áp dụng:

Các đơn vị thuộc Trường Cao đẳng Y tế Khánh Hòa và cán bộ, công chức, viên chức, người lao động của nhà trường.

Điều 2. Giải thích từ ngữ

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

1. "An toàn thông tin": Thông tin và hệ thống thông tin không bị truy cập, sử dụng, tiết lộ, gián đoạn, sửa đổi, phá hoại trái phép.

2. "Hệ thống thông tin": Tập hợp thiết bị phần cứng, phần mềm và cơ sở dữ liệu của các đơn vị phục vụ tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin.

3. "Mạng nội bộ": Mạng máy tính trong phạm vi Trường Cao đẳng Y tế Khánh Hòa;

4. "Mã độc": 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. "Rủi ro an toàn thông tin": Khả năng mất an toàn thông tin.

6. "Sự cố an toàn thông tin": Sự kiện mất an toàn thông tin.

7. "Mật khẩu phức tạp": Mật khẩu đáp ứng các yêu cầu sau:

a) Có tối thiểu 8 ký tự.

b) Gồm tối thiểu 3 trong 4 loại ký tự sau: chữ cái viết hoa (A - Z); chữ cái viết thường (a - z); chữ số (0 - 9); các ký tự khác trên bàn phím máy tính (` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? /) và dấu cách.

8. "Bí mật nhà nước": Tin về vụ, việc, tài liệu, vật, địa điểm, thời gian, lời nói có nội dung quan trọng ....theo quy định về tài liệu, thông tin mật của nhà nước.

9. "Người dùng": Cán bộ, công chức, viên chức, người lao động của các đơn vị sử dụng máy tính để xử lý công việc.

10. "Đơn vị" : các Phòng, Khoa, Bộ môn trực thuộc Ban Giám hiệu và các Bộ môn trực thuộc Khoa.

Điều 3. Nguyên tắc chung về đảm bảo an toàn thông tin

1. Đảm bảo an toàn thông tin là yêu cầu bắt buộc trong quá trình tạo lập, xử lý, sử dụng thông tin và thiết kế, xây dựng, vận hành, nâng cấp, hủy bỏ hệ thống thông tin.

2. Đơn vị, người dùng thực hiện các công đoạn liên quan đến thông tin nêu tại khoản 1 điều này có trách nhiệm đảm bảo an toàn thông tin theo quy định của Nhà nước, hướng dẫn của cơ quan, đơn vị có thẩm quyền trong lĩnh vực đảm bảo an toàn thông tin.

3. Người dùng có kiến thức chung về an toàn thông tin trên môi trường máy tính, mạng máy tính và có kiến thức cơ bản về an toàn thông tin phù hợp với công việc được phân công.

4. Bí mật nhà nước phải được bảo vệ theo quy định của Nhà nước về công tác bảo vệ bí mật nhà nước.

Điều 4. Những hành vi bị nghiêm cấm

1. Vi phạm các quy định về quản lý, vận hành và sử dụng mạng của Trường gây rối loạn hoạt động của hệ thống, trong đó bao gồm các hành vi: tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập không dây của cá nhân vào mạng nội bộ.

2. Can thiệp trái phép, gây nguy hại, xóa, thay đổi, sửa chữa, làm sai lệch thông tin trên mạng.

3. Phát tán thư rác, mã độc, thiết lập hệ thống thông tin giả mạo, lừa đảo trong mạng của nhà trường; lợi dụng điểm yếu của hệ thống thông tin để tấn công, chiếm quyền điều khiển trái phép đối với hệ thống.

4. Làm mất tác dụng của biện pháp an toàn thông tin do đơn vị thiết lập, trong đó bao gồm các hành vi: 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.

5. Lợi dụng mạng để truyền bá thông tin, quan điểm, thực hiện các hành vi gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội; phá hoại khối đại đoàn kết toàn dân; tuyên truyền chiến tranh xâm lược, khủng bố; gây thù hận, mâu thuẫn giữa các dân tộc, sắc tộc, tôn giáo.

6. Lợi dụng mạng để truyền bá trái phép tài liệu, hình ảnh, âm thanh hoặc dạng thông tin khác nhằm kích động bạo lực, dâm ô, đồi trụy, tội ác, tệ nạn xã hội, mê tín dị đoan, phá hoại thuần phong, mỹ tục của dân tộc; bôi nhọ, gây thù hận, xâm hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân.

7. Vi phạm quy định công tác bảo vệ bí mật nhà nước trong quá trình sử dụng hệ thống thông tin, trong đó bao gồm hành vi đánh cắp mật khẩu tài khoản truy cập hệ thống thông tin công vụ của người khác hoặc tiết lộ mật khẩu của bản thân cho đối tượng không được phép sử dụng.

Chương II
QUY ĐỊNH CỤ THỂ

Điều 5. Đảm bảo an toàn mức vật lý

1. Các khu vực sau phải được kiểm soát truy cập vật lý để phòng tránh truy cập trái phép hoặc sai mục đích: Trung tâm dữ liệu; khu vực chứa máy chủ và thiết bị lưu trữ; tủ mạng và đấu nối; thiết bị nguồn điện và dự phòng điện khẩn cấp; phòng vận hành, kiểm soát, quản trị hệ thống.

2. Thiết bị thuộc hệ thống máy chủ phải được bảo dưỡng định kỳ và duy trì chế độ bảo hành liên tục hoặc có cơ chế sửa chữa, thay thế đáp ứng yêu cầu về mức độ sẵn sàng của hệ thống trong suốt thời gian sử dụng.

Điều 6. Đảm bảo an toàn máy tính phục vụ công việc

1. Máy tính phục vụ công việc (bao gồm máy chủ, máy quản trị và máy tính phục vụ công việc của người dùng tại đơn vị):

a) Máy tính phục vụ công việc chỉ được cài đặt phần mềm theo danh mục phần mềm do nhà trường quy định hoặc được cung cấp theo các chương trình ứng dụng công nghệ thông tin của các cơ quan Nhà nước có thẩm quyền, được cập nhật bản vá lỗi hệ điều hành về an ninh, cài đặt phần mềm phòng diệt mã độc và cập nhật mẫu mã độc gần nhất.

b) Phòng Công nghệ thông tin chịu trách nhiệm cài đặt phần mềm cho máy tính phục vụ công việc. Người dùng không được can thiệp vào các phần mềm đã cài đặt trên máy tính (thay đổi, gỡ bỏ,...) khi chưa được sự đồng ý của Phòng Công nghệ thông tin.

c) Người dùng phải thực hiện thao tác khoá máy tính (sử dụng tính năng có sẵn trên máy) khi rời khỏi nơi đặt máy tính; tắt máy tính khi rời khỏi cơ quan.

2. Máy tính do cá nhân tự trang bị phải đáp ứng đầy đủ các điều kiện dưới đây khi kết nối vào hệ thống mạng nhà trường:

a) Cài đặt phần mềm phòng diệt mã độc và cập nhật mẫu mã độc gần nhất.

b) Không cài đặt phần mềm, công cụ có tính năng gây mất an toàn thông tin hoặc tạo rủi ro cho hệ thống mạng (cấp phát địa chỉ mạng, dò quét mật khẩu, dò quét cổng mạng, giả lập tấn công,..).

3. Người dùng 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 ngoài, băng từ) để lưu thông tin thuộc phạm vi bảo vệ quy định tại Điều 1 có trách nhiệm bảo vệ các thiết bị này và thông tin lưu trên thiết bị, tránh làm mất, lộ thông tin.

4. Thiết bị xử lý thông tin của đơn vị khi mang đi bảo hành, bảo dưỡng, sửa chữa, phải tháo ổ cứng khỏi thiết bị hoặc xóa thông tin, dữ liệu lưu trữ trên thiết bị (trừ trường hợp mang thiết bị đi khôi phục dữ liệu).

Điều 7. Đảm bảo an toàn, bảo mật thông tin

1. Nội dung mật, quan trọng hoặc nhạy cảm khi lưu trữ trên thiết bị di động hoặc truyền nhận trên hệ thống mạng phải được mã hoá, trong đó:

a) Bí mật nhà nước phải được mã hoá và được cấp có thẩm quyền chấp nhận sử dụng.

b) Văn bản điện tử có nội dung cần hạn chế tiếp cận nhưng không thuộc danh mục bí mật Nhà nước được sử dụng tính năng mã hoá (đặt mật khẩu) của các ứng dụng văn phòng (phần mềm soạn thảo, đọc văn bản, nén tệp).

2. Người dùng thực hiện soạn thảo, gửi, nhận dữ liệu có trách nhiệm xác định mức độ mật, nhạy cảm của dữ liệu để thực hiện phương thức bảo vệ dữ liệu phù hợp hoặc yêu cầu Phòng Công nghệ thông tin hướng dẫn, hỗ trợ phương thức bảo vệ trong trường hợp cần thiết.

3. Chỉ sử dụng hệ thống thư điện tử và các công cụ trao đổi thông tin do nhà trường cung cấp để trao đổi thông tin, tài liệu làm việc.

Điều 8. Sao lưu, dự phòng sự cố

1. Đơn vị phải chủ động sao lưu dữ liệu phòng ngừa sự cố; định kỳ thực hiện và kiểm tra dữ liệu sao lưu và chịu trách nhiệm đối với dữ liệu được sao lưu.

2. Đối với hệ thống máy chủ, Phòng Công nghệ thông tin đề xuất Ban Giám hiệu biện pháp dự phòng về thiết bị, phần mềm để đảm bảo sự hoạt động liên tục của hệ thống.

Chương III
TỔ CHỨC THỰC HIỆN

Điều 9. Trách nhiệm của các đơn vị và người dùng

1. Trách nhiệm của Phòng Công nghệ thông tin:

a) Chịu trách nhiệm đảm bảo an toàn thông tin của Nhà trường;

b) Tham mưu Ban Giám hiệu ban hành quy trình nội bộ triển khai đảm bảo an toàn thông tin;

c) Thực hiện việc giám sát, đánh giá, báo cáo Ban Giám hiệu các rủi ro mất an toàn thông tin và mức độ nghiêm trọng của các rủi ro đó;

d) Phối hợp với các cá nhân, đơn vị có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn, an ninh thông tin.

2. Trách nhiệm của người dùng và các đơn vị khác:

a) Nghiêm túc chấp hành các quy định, quy trình nội bộ, Quy định này và các quy định khác của pháp luật về an toàn thông tin. Chịu trách nhiệm đảm bảo an toàn thông tin trong phạm vi trách nhiệm và quyền hạn được giao;

b) Mỗi cán bộ, viên chức và người lao động phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp các thiết bị trên máy tính; không được vào các trang web không rõ về nội dung; không tải và cài đặt các phần mềm không rõ nguồn gốc, không liên quan đến công việc chuyên môn; không nhấp chuột vào các đường dẫn lạ không rõ về nội dung;

c) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin phải báo cáo ngay với Trưởng/Phó đơn vị và Phòng Công nghệ thông tin để kịp thời ngăn chặn và xử lý;

d)Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin do nhà trường hoặc Sở Thông tin và truyền thông tổ chức, cử đi.

Điều 10. Xử lý vi phạm

Mọi vi phạm về công tác đảm bảo an toàn thông tin nhà trường đều xử lý theo Quy chế thi đua khen thưởng của nhà trường và các văn bản nhà nước hiện hành.

Điều 11. Trách nhiệm thi hành

1. Các đơn vị, cán bộ, viên chức, người lao động của Nhà trường chịu trách nhiệm thi hành Quy định này.

2. Trưởng, Phó các đơn vị thuộc trường có trách nhiệm quán triệt, chỉ đạo và giám sát cán bộ, viên chức, người lao động thuộc đơn vị mình thực hiện đúng nội dung Quy định này.

3. Trong quá trình tổ chức thực hiện, nếu có những vấn đề khó khăn, vướng mắc, các đơn vị, cá nhân cần phản ánh ngay với phòng CNTT để tổng hợp, báo cáo Nhà trường xem xét, sửa đổi, bổ sung cho phù hợp./.

Nơi nhận:
- Như điều 3;
- Đảng ủy Trường;
- Ban Giám hiệu;
- Lưu : VT, P.CNTT;

HIỆU TRƯỞNG

Vũ Viết Sơn