

Số: 63 /QĐ-SYT

Thái Bình, ngày 14 tháng 02 năm 2017

QUYẾT ĐỊNH
Ban hành Quy định về việc đảm bảo an toàn thông tin
trên môi trường máy tính và mạng máy tính trong
cơ quan Sở Y tế Thái Bình, năm 2017

GIÁM ĐỐC SỞ Y TẾ THÁI BÌNH

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

Căn cứ Nghị định số 33/2002/NĐ-CP ngày 28/3/2002 của Chính phủ về việc quy định chi tiết thi hành Pháp lệnh bảo vệ bí mật Nhà nước;

Căn cứ Quyết định số 997/QĐ-UBND ngày 12/5/2009 của UBND tỉnh Thái Bình về chức năng, nhiệm vụ, quyền hạn và tổ chức bộ máy của Sở Y tế;

Xét đề nghị của Trưởng phòng Kế hoạch tài chính,

QUYẾT ĐỊNH:

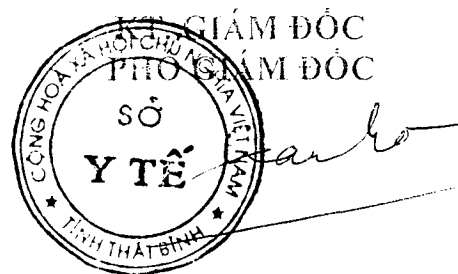
Điều 1. Ban hành kèm theo Quyết định này Quy định về việc đảm bảo an toàn thông tin trên môi trường máy tính và mạng máy tính trong cơ quan Sở Y tế Thái Bình.

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

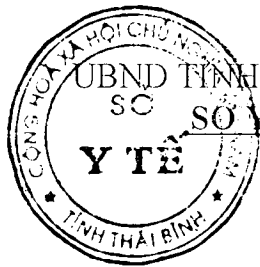
Điều 3. Chánh văn phòng, Chánh thanh tra, Trưởng các phòng, ban thuộc Sở Y tế, công chức, viên chức Sở Y tế, các tổ chức và cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:

- GD, PGD Sở;
- Các phòng, ban thuộc Sở;
- Lưu: VT, KHTC.



Trần Quang Hải



UBND TỈNH THÁI BÌNH
SỞ Y TẾ

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

QUY ĐỊNH

Về việc đảm bảo an toàn thông tin
trên môi trường máy tính và mạng máy tính trong cơ quan Sở Y tế
(Kèm theo Quyết định số 63 /QĐ-SYT ngày 14 tháng 02 năm 2017
của Giám đốc Sở Y tế)

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 và các hệ thống có khả năng tiếp cận thông tin số của Sở Y tế. Thông tin được đảm bảo an toàn bao gồm tất cả các loại thông tin của Sở Y tế, thông tin do các cơ quan, tổ chức khác gửi đến Sở Y tế.

2. Đối tượng áp dụng:

a) Cán bộ, công chức, viên chức, nhân viên của các phòng, ban của Sở Y tế: áp dụng đầy đủ quy định này.

b) Tổ chức, cá nhân có kết nối vào mạng nội bộ của Sở Y tế: áp dụng quy định này trong hoạt động trao đổi thông tin và sử dụng các ứng dụng của Sở Y tế.

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 thuộc ngành Y tế phục vụ tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin.

3. “Hệ thống quan trọng”: Hệ thống thông tin có ảnh hưởng lớn tới hoạt động của các đơn vị thuộc ngành Y tế và lợi ích công cộng.

4. “Mạng nội bộ”: Mạng máy tính trong phạm vi trụ sở của Sở Y tế.

5. “Hạ tầng truyền thông thống nhất ngành Y tế”: Mạng diện rộng kết nối các mạng nội bộ của các đơn vị thuộc ngành Y tế.

6. “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.

7. “Điểm yếu”: Điểm có thể bị khai thác gây mất an toàn thông tin; còn được gọi là “lỗ hổng bảo mật”.

8. “Rủi ro an toàn thông tin”: Khả năng mất an toàn thông tin.

9. “Sự cố an toàn thông tin”: Sự kiện mất an toàn thông tin.

10. “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.

11. “Thuật toán mã hoá an toàn”: Thuật toán mã hoá theo tiêu chuẩn Việt Nam hoặc thế giới mà tại thời điểm áp dụng chưa có công bố thuật toán đó đã bị giải hoặc nếu có khả năng giải thì thời gian giải thuật toán này dài hơn thời gian dữ liệu cần được bảo vệ dưới dạng mã hoá.

12. “Bí mật nhà nước”: Tin về vụ, việc, tài liệu, vật, địa điểm, thời gian, lời nói có nội dung quan trọng thuộc lĩnh vực chính trị, quốc phòng, an ninh, đối ngoại, kinh tế, khoa học, công nghệ, các lĩnh vực khác mà Nhà nước không công bố hoặc chưa công bố và nếu bị tiết lộ thì gây nguy hại cho Nhà nước Cộng hoà xã hội chủ nghĩa Việt Nam.

Bí mật nhà nước được quy định cụ thể tại Pháp lệnh Bảo vệ bí mật nhà nước và các văn bản quy định, hướng dẫn triển khai thực hiện Pháp lệnh.

13. “Người dùng”: Cán bộ, công chức, viên chức, nhân viên của các đơn vị thuộc Sở Y tế sử dụng máy tính để xử lý công việc, các cán bộ thuộc ngành Y tế có sử dụng hệ thống mạng văn phòng điện tử liên thông.

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, của Bộ Y tế và hướng dẫn của cơ quan, đơn vị có thẩm quyền trong lĩnh vực đảm bảo an toàn thông tin.

3. Người dùng phải được tập huấn kiến thức chung về an toàn thông tin trên môi trường máy tính, mạng máy tính và kiến thức nâng cao 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 và của ngành Y tế về công tác bảo vệ bí mật nhà nước và các nội dung tương ứng trong quy định này.

Điều 4. Những hành vi bị nghiêm cấm

1. Vi phạm các quy định về quản lý, vận hành và sử dụng mạng của ngành Y tế gây rối loạn hoạt động của hệ thống, trong đó bao gồm các hành vi: tự ý đầu 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; 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 (modem quay số, USB 3G, điện thoại di động, máy tính bảng).

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 ngành Y tế; 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, tháo 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 của ngành Y tế 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 ngành Y tế 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; thiết bị lưu trữ; tủ mạng và đầu 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 quan trọng 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.

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. Không mang ra nước ngoài thông tin của cơ quan, Nhà nước không liên quan tới nội dung công việc thực hiện ở nước ngoài.

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). Thiết bị lưu trữ không sử dụng tiếp cho công việc của đơn vị (thanh lý, cho, tặng) phải được xóa nội dung bằng phần mềm hoặc bằng thiết bị hủy dữ liệu chuyên dụng hay phá hủy vật lý.

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 đơn vị quy định và do bộ phận công nghệ thông tin của đơn vị quản lý hoặc được cung cấp theo các chương trình ứng dụng công nghệ thông tin của Sở Y tế và các cơ quan Nhà nước khác 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) Bộ phận công nghệ thông tin của đơn vị 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 bộ phận công nghệ thông tin của đơn vị.

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 của ngành Y tế:

- a) Cài đặt đầy đủ các bản vá lỗi hệ điều hành về an ninh.
- b) Cài đặt phần mềm phòng diệt mã độc và cập nhật mẫu mã độc gần nhất.
- c) 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...).

Điều 7. Đảm bảo an toàn hệ thống mạng máy tính

1. Kết nối mạng diện rộng phải được thiết lập và vận hành theo Quy chế quản lý, vận hành và sử dụng mạng văn phòng điện tử liên thông ban hành tại Quyết định số 20/2012/QĐ-UBND ngày 19/12/2012 của UBND tỉnh Thái Bình và các văn bản sửa đổi, cập nhật quy chế này nếu có.

2. Hệ thống mạng không dây (nếu có) phải đáp ứng các điều kiện tối thiểu sau:

- a) Thiết bị phần cứng phải có chứng nhận Wi-Fi (chứng nhận của Liên minh Wi-Fi (www.wi-fi.org) cho sản phẩm đạt tiêu chuẩn 802.11).
- b) Áp dụng mã hoá dữ liệu truyền nhận sử dụng thuật toán mã hoá an toàn.
- c) Người dùng mạng không dây phải được cung cấp định danh duy nhất và xác thực qua kênh mã hoá.
- d) Các điểm truy cập không dây (thiết bị phát sóng làm cầu nối giữa mạng có dây và không dây) của đơn vị được bảo vệ tránh bị tiếp cận trái phép.

3. Đối với truy cập từ xa vào hệ thống mạng nội bộ:

- a) Máy tính dùng để kết nối tới mạng của đơn vị phải được đảm bảo an toàn theo quy định tại Điều 6.
- b) Kết nối truy cập từ xa phải sử dụng mã hoá kênh truyền theo tiêu chuẩn mã hóa do Bộ Thông tin và Truyền thông quy định.
- c) Truy cập từ xa cho mục đích quản trị hệ thống phải áp dụng xác thực tối thiểu 2 yếu tố.
- d) Hạn chế truy cập từ xa vào mạng nội bộ từ những điểm truy cập Internet công cộng.

4. Các thành phần tham gia vào hệ thống mạng của đơn vị phải được đồng bộ với một nguồn thời gian thống nhất trong đơn vị và theo quy chuẩn quốc tế GMT +7.

Điều 8. Đảm bảo an toàn kết nối Internet

1. Các phòng, ban thuộc Sở Y tế áp dụng các biện pháp cần thiết để đảm bảo an toàn thông tin trong hoạt động kết nối Internet, tối thiểu đáp ứng yêu cầu sau:

a) Có tường lửa kiểm soát truy cập Internet.

b) Lọc bỏ, không cho phép truy cập các trang tin có nghi ngờ chứa mã độc hoặc các nội dung không phù hợp (phản động hoặc trái thuần phong mỹ tục).

2. Đối với thiết bị công nghệ thông tin khác, chỉ thiết lập kết nối Internet cho các hệ thống cần phải có giao tiếp với Internet (các máy chủ, thiết bị cung cấp giao diện ra Internet của trang tin điện tử, dịch vụ công, thư điện tử; thiết bị cập nhật bản vá hệ điều hành, mẫu mã độc, mẫu điểm yếu, mẫu tấn công).

Điều 9. Đảm bảo an toàn mức ứng dụng

1. Yêu cầu về đảm bảo an toàn thông tin phải được đưa vào tất cả các công đoạn liên quan đến ứng dụng (thiết kế, xây dựng, triển khai và vận hành, sử dụng).

2. Ứng dụng do đơn vị phát triển hoặc thuê phát triển phải đáp ứng yêu cầu sau:

a) Mã hoá thông tin bí mật hoặc nhạy cảm theo quy định tại Điều 10.

b) Kiểm tra tính hợp lệ của dữ liệu đầu vào và đầu ra để đảm bảo dữ liệu chính xác và phù hợp.

c) Giới hạn số lần đăng nhập sai liên tiếp vào ứng dụng.

d) Thực hiện quy trình kiểm soát việc cài đặt phần mềm trên các máy chủ, máy tính của người dùng, thiết bị mạng đang hoạt động thuộc hệ thống mạng nội bộ, đảm bảo các phần mềm khi cài đặt trong hệ thống có nguồn gốc an toàn, không bị nhiễm mã độc.

đ) Hạn chế truy cập tới mã nguồn chương trình và phải đặt mã nguồn trong môi trường an toàn do bộ phận chuyên trách quản lý.

e) Kiểm tra phát hiện và khắc phục điểm yếu của ứng dụng trước khi đưa vào sử dụng và trong quá trình sử dụng (khi có thông tin xuất hiện điểm yếu mới trên môi trường hoạt động của ứng dụng; tối thiểu mỗi năm một lần).

3. Đối với ứng dụng mua ở dạng đóng gói:

a) Theo dõi, nắm bắt thông tin về các điểm yếu được phát hiện và cập nhật thường xuyên bản vá lỗi về an ninh cho ứng dụng.

b) Trường hợp điểm yếu đã được phát hiện mà chưa có bản vá lỗi của đơn vị sản xuất phần mềm, phải thực hiện đánh giá rủi ro và có biện pháp phòng tránh phù hợp.

Điều 10. Đảm bảo an toàn mức dữ liệu

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 của ngành Y tế phải được mã hoá bằng giải pháp do Ban Cơ yếu Chính phủ cung cấp hoặc được cấp có thẩm quyền chấp nhận sử dụng trong ngành Y tế

b) Áp dụng mã hoá kênh kết nối cho các hoạt động sau theo tiêu chuẩn mã hóa do Bộ Thông tin và Truyền thông quy định: quản trị hệ thống; đăng nhập mạng, ứng dụng; gửi nhận dữ liệu tự động giữa các máy chủ; nhập và biên tập dữ liệu; tra cứu dữ liệu mật, nhạy cảm.

c) Khuyến khích áp dụng công nghệ chữ ký số để xác thực và bảo mật dữ liệu, đặc biệt trong trường hợp cần đảm bảo chống từ chối nguồn gốc dữ liệu.

d) 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), nhưng phải sử dụng thuật toán mã hoá an toàn.

2. Cá nhân 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 bộ phận 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 đơn vị quản lý trực tiếp, hoặc các cơ quan Nhà nước, các tổ chức có thẩm quyền cung cấp để trao đổi thông tin, tài liệu làm việc. Không sử dụng các phương tiện trao đổi thông tin công cộng trên Internet cho mục đích này.

Điều 11. Đảm bảo an toàn trong hoạt động trao đổi thông tin với các tổ chức, cá nhân ngoài ngành Y tế

1. Tổ chức, cá nhân thuộc phạm vi quy định tại điểm c và điểm d khoản 2 Điều 1 phải cam kết bảo mật thông tin của ngành Y tế mà tổ chức, cá nhân đó sẽ tiếp xúc trước khi bắt đầu thực hiện công việc theo hợp đồng, thoả thuận giữa hai bên.

2. Khi trao đổi các thông tin cần bảo mật của ngành Y tế qua hệ thống mạng phải mã hoá theo quy định tại Điều 10 của quy định này. Khi trao đổi bí mật nhà nước phải thực hiện theo quy định về công tác bảo vệ bí mật nhà nước của ngành Y tế.

3. Đối với tổ chức, cá nhân bên ngoài có thiết lập kết nối vào mạng của ngành Y tế:

a) Phải phân tích rủi ro về an toàn thông tin trước khi kết nối mạng và có biện pháp kiểm soát các rủi ro này.

b) Thỏa thuận bằng văn bản giữa các bên về các điều kiện cụ thể mà tổ chức, cá nhân bên ngoài phải đáp ứng khi kết nối vào mạng của ngành Y tế; kiểm tra định kỳ việc thực hiện thỏa thuận này.

Điều kiện tổ chức, cá nhân bên ngoài phải đáp ứng tối thiểu bao gồm: vùng mạng của tổ chức, cá nhân bên ngoài được sử dụng để kết nối vào mạng của ngành Y tế phải được kiểm soát bằng tường lửa; các máy tính trong phân đoạn mạng này phải được cập nhật bản vá hệ điều hành, mẫu phòng diệt mã độc; các tài khoản truy cập hệ thống tối thiểu phải áp dụng mật khẩu phức tạp; chỉ được kết nối Internet trong trường hợp kết nối này phục vụ công việc của ngành Y tế.

Điều 12. Sao lưu, dự phòng sự cố

1. Đơn vị phải có thiết bị, quy trình, nhân sự phục vụ công tác sao lưu dữ liệu phòng ngừa sự cố; định kỳ kiểm tra dữ liệu sao lưu và phục hồi thử hệ thống từ dữ liệu sao lưu; quản lý, bảo quản phương tiện sao lưu phòng tránh hỏng, mất dữ liệu sao lưu.

2. Đối với hệ thống quan trọng, đơn vị phải có biện pháp dự phòng về thiết bị, phần mềm để đảm bảo sự hoạt động liên tục của hệ thống.

Điều 13. Tài khoản công nghệ thông tin

1. Tài khoản người dùng:

a) Mỗi người dùng khi sử dụng hệ thống thông tin phải được cấp và sử dụng tài khoản truy cập với định danh duy nhất 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 có trách nhiệm quản lý tài khoản.

b) Tài khoản của người dùng không được có quyền quản trị trên máy tính nối mạng. Tài khoản quản trị máy tính chỉ được sử dụng trong trường hợp cài đặt phần mềm trên máy tính. Tài khoản quản trị máy tính để bàn phải do bộ phận công nghệ thông tin của đơn vị nắm giữ. Đối với máy tính xách tay, người dùng phải được hướng dẫn sử dụng đúng cách tài khoản quản trị máy tính và có trách nhiệm thực hiện theo đúng hướng dẫn.

c) Trường hợp người dùng thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ hưu phải thông báo kịp thời cho bộ phận quản lý tài khoản công nghệ thông tin để thực hiện điều chỉnh, thu hồi, hủy bỏ các quyền sử dụng của người dùng đối với hệ thống mạng, ứng dụng. Quy định cụ thể như sau:

- Văn bản quyết định về việc bổ nhiệm chức vụ lãnh đạo, thay đổi vị trí công tác, chuyển công tác, thôi việc, nghỉ hưu phải ghi tên bộ phận chịu trách nhiệm quản lý tài khoản công nghệ thông tin tại phần ghi nơi nhận của văn bản. Trường hợp thay đổi vị trí công tác không sử dụng hình thức văn bản quyết định, đơn vị quản lý người dùng phải thông báo cho bộ phận quản lý tài khoản công nghệ thông tin bằng công văn hoặc theo cách thức quy định trong quy trình quản lý tài khoản công nghệ thông tin áp dụng tại đơn vị.

- Tài khoản công nghệ thông tin phải được điều chỉnh, thu hồi, hủy bỏ trong thời gian không quá 03 ngày làm việc tính từ ngày người dùng chính thức chuyển công tác ra khỏi ngành Y tế, thôi việc, nghỉ hưu; không quá 05 ngày làm việc trong trường hợp thay đổi vị trí công tác trong nội bộ đơn vị hoặc chuyển công tác tới đơn vị khác thuộc ngành Y tế.

- Phải có văn bản đề nghị của đơn vị quản lý người dùng trong trường hợp cần duy trì tài khoản của người dùng sau thời điểm người dùng chính thức thay đổi vị trí công tác, chuyển công tác, thôi việc, nghỉ hưu; trong đó nêu rõ lý do, các quyền sử dụng cần duy trì và thời gian duy trì.

2. Tài khoản quản trị hệ thống (thiết bị, mạng, hệ điều hành, ứng dụng, cơ sở dữ liệu) phải tách biệt với tài khoản truy cập mạng, ứng dụng với tư cách người dùng thông thường. Tài khoản quản trị hệ thống phải được giao đích danh cá nhân làm công tác quản trị hệ thống. Hạn chế dùng chung tài khoản quản trị.

3. Phương tiện xác thực tài khoản:

a) Mật khẩu phức tạp phải được áp dụng cho tất cả các tài khoản truy cập, sử dụng, quản trị hệ thống.

b) Đổi mật khẩu ngay 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; đổi mật khẩu tối thiểu 03 tháng một lần đối với tài khoản của người dùng và 02 tháng một lần đối với tài khoản quản trị hệ thống.

c) Người dùng, người làm công tác quản trị hệ thống có trách nhiệm bảo vệ thông tin tài khoản được cấp.

4. Rà soát tối thiểu mỗi năm một lần các tài khoản đang cấp trên hệ thống, đảm bảo các tài khoản và quyền truy cập hệ thống được cấp phát đúng.

Điều 14. Đảm bảo an toàn trong công tác vận hành hệ thống

1. Quản trị hệ thống:

a) Máy tính dùng để quản trị hệ thống chỉ được cài đặt phần mềm cần thiết cho hoạt động quản trị hệ thống, đặt trong vùng mạng phục vụ công tác quản trị hệ thống và chỉ được cấp quyền truy cập cho các cá nhân được giao trách nhiệm quản trị hệ thống.

b) Đổi tên tài khoản mặc định (nếu có thể) và mật khẩu mặc định của quản trị hệ thống khi hệ thống được thiết lập.

c) Sử dụng kênh trao đổi thông tin an toàn (có mã hoá) cho truy cập quản trị hệ thống.

2. Thực hiện quản lý cấu hình hệ thống quan trọng: Quản lý thông tin về thông số kỹ thuật, mục đích sử dụng, vị trí lắp đặt, nguồn cung cấp, thời gian sử dụng, bảo hành, bảo dưỡng; đảm bảo thông tin sẵn dụng khi có yêu cầu (phục vụ công tác đánh giá năng lực, tính sẵn sàng, an toàn của hệ thống, công tác mua sắm, bảo dưỡng, bảo hành).

3. Thực hiện quản lý thay đổi đối với hệ thống quan trọng: Xác định mức độ cần thiết của thay đổi, ảnh hưởng tiềm ẩn (các sự cố có thể xảy ra, phạm vi tác động) và biện pháp phòng tránh (bao gồm thủ tục hủy bỏ thay đổi và khôi phục hệ thống khi thay đổi không thành công), xác định thời gian thực hiện phù hợp; phê duyệt kế hoạch thay đổi; thông báo cho các bên liên quan về kế hoạch và kết quả của thay đổi.

4. Thực hiện quản lý năng lực hệ thống quan trọng: Giám sát hiệu năng và thực hiện các biện pháp cần thiết (dọn dẹp hệ thống, điều chỉnh thông số kỹ thuật, bổ sung mua sắm) để đảm bảo khả năng xử lý và tính sẵn sàng của hệ thống theo yêu cầu.

5. Kiểm tra, đảm bảo nhật ký hệ thống của các thành phần thuộc hệ thống quan trọng được lưu liên tục tối thiểu trong 03 tháng gần nhất và sẵn sàng sử dụng cho công tác phân tích sự cố an toàn thông tin.

Điều 15. Quản lý an toàn thông tin

1. Đơn vị phải phân công nhân sự quản lý an toàn thông tin trên môi trường máy tính và mạng máy tính (bao gồm công tác giám sát, kiểm tra việc thực hiện quy định này tại đơn vị).

2. Các hệ thống an ninh mạng (cập nhật bản vá hệ điều hành, phòng diệt mã độc, tường lửa, phát hiện và phòng chống tấn công...) phải được giám sát thường xuyên để đảm bảo tác dụng của hệ thống, đồng thời phát hiện và xử lý sớm các vấn đề về an toàn thông tin. Thực hiện kết xuất định kỳ hàng tháng hoặc hàng quý các báo cáo từ hệ thống an ninh mạng để theo dõi, đánh giá các vấn đề của hệ thống.

3. Thực hiện quản lý rủi ro an toàn thông tin: Xác định các rủi ro an toàn thông tin đối với thông tin, dữ liệu và các hệ thống quan trọng của đơn vị; phân tích, đánh giá các rủi ro này và nghiên cứu, triển khai các biện pháp khắc phục phù hợp. Thực hiện công tác này mỗi khi đơn vị có thay đổi về nhu cầu bảo vệ thông tin, thay đổi trong hệ thống công nghệ thông tin của đơn vị hoặc khi xuất hiện các nguy cơ mất an toàn thông tin mới hoặc tối thiểu mỗi năm một lần.

4. Thực hiện quản lý sự cố an toàn thông tin: Thiết lập quy trình báo cáo sự cố an toàn thông tin cho các cấp quản lý thuộc đơn vị; phân tích, xác định nguyên nhân của sự cố, biện pháp khắc phục và ngăn ngừa tái diễn; tổng hợp thông tin về các sự cố trong báo cáo an toàn thông tin định kỳ của đơn vị.

5. Người dùng phải được bộ phận công nghệ thông tin của đơn vị hướng dẫn, hỗ trợ, cung cấp các công cụ cần thiết để thực hiện trách nhiệm đảm bảo an toàn thông tin theo quy định.

Chương III TỔ CHỨC THỰC HIỆN

Điều 16. Trách nhiệm của các đơn vị

1. Phòng Kế hoạch tài chính:

a) Tổ chức phổ biến và triển khai thực hiện quy định này tại cơ quan Sở Y tế và các đơn vị có kết nối vào mạng nội bộ cơ quan Sở Y tế.

b) Trình Lãnh đạo Sở Y tế phê duyệt và tổ chức triển khai kế hoạch ứng phó trong tình huống khẩn cấp (phát hiện có tấn công đánh cắp bí mật nhà nước của ngành Y tế qua đường mạng, các hệ thống quan trọng của ngành Y tế bị chiếm quyền điều khiển).

c) Hướng dẫn, kiểm tra việc thực hiện quy định này của các phòng ban thuộc Sở Y tế, các đơn vị có kết nối trao đổi thông tin với mạng nội bộ cơ quan Sở Y tế.

d) Tổng hợp, báo cáo Sở Y tế theo định kỳ hàng quý về công tác đảm bảo an toàn thông tin của toàn ngành Y tế theo nội dung của quy định này và các vấn đề về an toàn thông tin phát sinh trong kỳ báo cáo.

e) Trình Sở Y tế sửa đổi, bổ sung quy định này để phù hợp với tình hình và điều kiện thực tế.

3. Các đơn vị tham gia sử dụng hệ thống mạng nội bộ cơ quan Sở Y tế:

a) Phối hợp với Phòng Kế hoạch tài chính – Sở Y tế trong việc triển khai, thực hiện quy định áp dụng cho đối tượng người dùng tại đơn vị.

b) Phối hợp với Sở Y tế triển khai kế hoạch ứng phó tấn công khẩn cấp về các nội dung liên quan tới đơn vị.

c) Phản ánh nhu cầu, vướng mắc trong quá trình triển khai, thực hiện đảm bảo an ninh thông tin tại đơn vị tới phòng Kế hoạch tài chính.

4. Cơ quan, tổ chức, cá nhân ngoài ngành Y tế có liên quan:

a) Tuân thủ quy định này, quy định công tác bảo vệ bí mật nhà nước của ngành Y tế, các cam kết, đảm bảo an toàn thông tin khi cung cấp dịch vụ công nghệ thông tin và thực hiện các hoạt động trao đổi thông tin với các phòng ban thuộc Sở Y tế. Trường hợp tham gia sử dụng ứng dụng của ngành Y tế, phải tuân thủ các yêu cầu, hướng dẫn, quy trình đảm bảo an toàn thông tin cụ thể của ứng dụng.

b) Phản ánh vướng mắc, nguy cơ, rủi ro ảnh hưởng đến an toàn thông tin của ngành Y tế phát hiện được trong quá trình làm việc đề nghị phản ánh về Sở Y tế để cùng phối hợp xử lý, giải quyết.

Điều 17. Trách nhiệm của cá nhân

1. Trưởng các phòng, ban thuộc Sở có trách nhiệm: phổ biến tới từng cán bộ, công chức, viên chức, nhân viên của phòng; thường xuyên kiểm tra việc thực hiện quy định này tại đơn vị; định kỳ hàng quý báo cáo Sở (qua phòng Kế hoạch Tài chính); chịu trách nhiệm trước pháp luật và Lãnh đạo Sở Y tế về các vi phạm, thất thoát thông tin, dữ liệu mật thuộc phạm vi quản lý của phòng, ban do không tổ chức, chỉ đạo, kiểm tra cán bộ của phòng, ban thực hiện đúng quy định.

2. Cán bộ, công chức, viên chức, nhân viên của Sở Y tế, các cá nhân thuộc đối tượng áp dụng của quy định có trách nhiệm: tuân thủ đúng quy định; thông báo các vấn đề bất thường liên quan tới an toàn thông tin cho bộ phận công nghệ thông tin của đơn vị; chịu trách nhiệm trước pháp luật và Lãnh đạo đơn vị về các vi phạm, thất thoát dữ liệu mật của ngành Y tế do không tuân thủ quy định.

3. Tập thể, cá nhân vi phạm quy định đảm bảo an toàn thông tin làm ảnh hưởng đến việc thực hiện nhiệm vụ chính trị của ngành Y tế hoặc gây phương hại đến an ninh quốc gia thì tùy theo tính chất, mức độ của hành vi vi phạm sẽ bị xử lý hành chính, xử lý kỷ luật hoặc truy cứu trách nhiệm hình sự. Nếu gây thiệt hại về tài sản thì phải bồi thường theo quy định của pháp luật./.

GIÁM ĐỐC
PHÓ GIÁM ĐỐC
SỞ
Y TẾ
THÀNH PHỐ HỒ CHÍ MINH
TRẦN QUANG HẢI

