SỞ Y TẾ BÌNH ĐỊNH
BỆNH VIỆN MẮT

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

Số: 469 /QĐ-BVM

Bình Định, ngày 28 tháng 09 năm 2018

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Bệnh viện Mắt Bình Định

GIÁM ĐỐC BỆNH VIỆN MẮT

Căn cứ Luật Công nghệ thông tin ngày 29/6/2006;

Căn cứ Luật An toàn thông tin mạng ngày 19/11/2015;

Căn cứ Quyết định số 22/QĐ-UBND ngày 12/7/2012 của UBND tỉnh Bình Định về việc ban hành Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan quản lý hành chính nhà nước tỉnh Bình Định;

Căn cứ Giấy phép số 01/GPTTĐT-STTTT ngày 28/9/2016 của Sở Thông tin và truyền thông về giấy phép thiết lập trang thông tin điện tử tổng hợp trên mạng;

Căn cứ Quyết định số 1590/QĐ-SYT ngày 20/10/2008 của Sở Y tế Bình Định về việc ban hành Quy chế tổ chức và hoạt động Bệnh viện Mắt Bình Định;

Theo đề nghị của Trưởng phòng TC-HC-TC Bệnh viện Mắt,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này "Quy chế bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Bệnh viện Mắt Bình Định".

Điều 3. Các Ông (Bà) phụ trách các khoa phòng thuộc Bệnh viện Mắt và các cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này kể từ ngày ký.

Nơi nhận:
- Như điều 3;
- Sở Y tế-báo cáo;
- Lưu: VT.

GIÁM ĐỐC

Nguyễn Thanh Triết

SỞ Y TẾ BÌNH ĐỊNH
BỆNH VIỆN MẮT

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

QUY CHẾ

Bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Bệnh viện Mắt Bình Định

(Kèm theo Quyết định số 469 /QĐ-BVM, ngày 28 tháng 9 năm 2018 của Bệnh viện Mắt Bình Định)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. Quy chế này quy định về bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Bệnh viện Mắt Bình Định.

2. Quy chế này áp dụng cho cán bộ, công chức, viên chức và người lao động thuộc Bệnh viện Mắt Bình Định.

Điều 2. Giải thích từ ngữ

1. An toàn, an ninh thông tin: Là sự bảo vệ thông tin và hệ thống thông tin 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 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 như: Hệ thống mạng nội bộ, hệ thống văn phòng điện tử, thư điện tử, trang thông tin điện tử,…

3. Xâm phạm an toàn, an ninh thông tin: Là hành vi truy nhập, sử dụng, tiết lộ, làm gián đoạn, sửa đổi, làm sai lệch chức năng, phá hoại trái phép thông tin hay hệ thống thông tin.

4. Nguy cơ mất an toàn, an ninh thông tin: Là những nhân tố bên trong hoặc bên ngoài có khả năng ảnh hưởng tới trạng thái an toàn thông tin.

5. Đánh giá rủi ro an toàn, an ninh thông tin: Là việc xác định, phân tích nguy cơ mất an toàn thông tin có thể có và dự báo mức độ, phạm vi ảnh hưởng và khả năng gây thiệt hại khi xảy ra sự cố mất an toàn thông tin.

6. Quản lý rủi ro an toàn, an ninh thông tin: Là việc thực hiện đánh giá rủi ro an toàn thông tin, xác định yêu cầu bảo vệ thông tin và hệ thống thông tin và áp dụng giải pháp phòng, chống, giảm thiểu thiệt hại khi có sự cố mất an toàn thông tin.

7. Hệ thống mạng LAN: Là hệ thống mạng nội bộ dùng để kết nối các máy tính trong phạm vi cơ quan, đơn vị. Các máy tính trong mạng LAN có thể chia sẻ tài nguyên với nhau như: chia sẻ tập tin, máy in, máy quét và một số thiết bị khác.

8. Phần mềm độc hại: Là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hoặc 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.

Điều 3. Các hành vi bị nghiêm cấm

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

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

3. Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của các biện pháp bảo vệ an toàn thông tin cho hệ thống thông tin; lợi dụng sơ hở, điểm yếu của hệ thống thông tin, tấn công, chiếm quyền điều khiển trái phép đối với hệ thống thông tin;

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

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, lợi ích quốc gia trên mạng; phá hoại khối đại đoàn kết toàn dân; tuyên truyền chiến tranh xâm lược, khủng bố; gây hận thù, mâu thuẫn giữa các dân tộc, sắc tộc, tôn giáo và bài ngoại;

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. Các hành vi bị nghiêm cấm khác theo quy định của pháp luật.

Chương II

BẢO ĐẢM AN TOÀN, AN NINH THÔNG TIN

Điều 4. Các biện pháp quản lý kỹ thuật cơ bản trong công tác bảo đảm an toàn, an ninh thông tin.

1. Tổ chức mô hình mạng: Cài đặt, cấu hình, tổ chức hệ thống mạng theo mô hình Máy khách/Máy chủ (Client/Server). Khi thiết lập các dịch vụ trên môi trường mạng Internet, chỉ cung cấp những chức năng thiết yếu nhất bảo đảm duy trì hoạt động của hệ thống thông tin; hạn chế sử dụng chức năng, cổng giao tiếp mạng, giao thức và các dịch vụ không cần thiết.

2. Quản lý hệ thống mạng không dây (Wireless LAN): Khi thiết lập mạng không dây, cần thiết lập các thông số an toàn và định kỳ thay đổi mật khẩu truy cập nhằm tăng cường công tác bảo mật.

3. Tổ chức quản lý tài khoản: Tiến hành rà soát định kỳ các tài khoản và định danh người dùng trong hệ thống thông tin. Hủy tài khoản, quyền truy nhập hệ thống thông tin, thu hồi lại tất cả các tài sản liên quan tới hệ thống thông tin (khóa, thẻ nhận dạng, thư mục lưu trữ,…) đối với cán bộ, công chức, viên chức, người lạo động không còn sử dụng.

4. Quản lý đăng nhập hệ thống: Các hệ thống thông tin cần giới hạn số lần đăng nhập vào hệ thống, tự động khóa tài khoản khi liên tục đăng nhập sai vượt quá số lần quy định. Tổ chức theo dõi, giám sát tất cả các phương pháp đăng nhập từ xa, nhất là các trường hợp đăng nhập vào hệ thống với mục đích quản trị. Tăng cường việc sử dụng mạng riêng ảo (VPN – Virtual Private Network) khi có nhu cầu làm việc từ xa; yêu cầu người sử dụng đặt lại mật khẩu với độ an toàn cao.

5. Quản lý nhật ký sự kiện (loglife): Hệ thống thông tin cần ghi nhận các sự kiện: quá trình đăng nhập hệ thống, các thao tác cấu hình hệ thống, quá trình truy xuất hệ thống… Thường xuyên kiểm tra, sao lưu (backup) các nhật ký sự kiện theo từng tháng để theo dõi, xác định những sự kiện đã xảy ra của hệ thống và hạn chế việc tràn nhật ký sự kiện gây ảnh hưởng đến hoạt động của hệ thống.

6. Chống phần mềm độc hại: Triển khai các phần mềm chống mã độc trên các máy tính, thiết bị di động trong mạng để phát hiện, loại trừ phần mềm độc hại.Thường xuyên cập nhật các phiên bản mới, các bản vá lỗi của các phần mềm chống virus để bảo đảm chương trình quét virus của cơ quan trên các máy chủ, máy trạm luôn được cập nhật mới nhất; thiết lập chế độ quét thường xuyên ít nhất tuần 01 lần. Thường xuyên cập nhật bản vá các lỗ hổng bảo mật của hệ điều hành và các phần mềm ứng dụng trên máy tính để hạn chế tối đa rủi ro mất an toàn thông tin.

7. Tổ chức quản lý tài nguyên: Kiểm tra, giám sát chức năng chia sẻ thông tin (Network File and Folder Sharing). Tổ chức cấp phát tài nguyên trên máy chủ theo danh mục thư mục cho từng khoa phòng; khuyến cáo người sử dụng cân nhắc việc chia sẻ tài nguyên trên máy đang sử dụng, tuyệt đối không được chia sẻ toàn bộ ổ cứng. Khi thực hiện việc chia sẻ tài nguyên trên máy chủ hoặc máy cục bộ cần sử dụng mât khẩu để bảo vệ thông tin.

8. Thiết lập cơ chế sao lưu và phục hồi cho máy chủ, máy trạm và hệ thống thông tin có liên quan: Máy chủ và máy trạm cần được thực hiện các biện pháp sao lưu dữ liêu, thông tin quan trọng nhằm phục vụ cho công tác phục hồi dữ liệu một cách nhanh nhất.

Điều 5. Các biện pháp quản lý vận hành trong công tác bảo đảm an toàn, an ninh thông tin

1. Đối với các khoa, phòng trong bệnh viện :

a) Thường xuyên phổ biến, hướng dẫn, trang bị các kiến thức, kỹ năng về an toàn thông tin cho cán bộ, công chức, viên chức để vận hành, khai thác, sử dụng các hệ thống thông tin một cách an toàn.

b) Không sử dụng máy tính có kết nối mạng Internet để đánh máy, in, lưu trữ tài liệu mật. Mọi thông tin thuộc bí mật nhà nước khi lưu trữ và truyền đi trên môi

trường mạng phải được mã hóa và quản lý theo quy định của pháp luật về cơ yếu, khuyến khích ứng dụng, sử dụng chữ ký số trong giao dịch điện tử.

c) Việc thanh lý, tiêu hủy thiết bị, phần mềm,vật mang thông tin của các cơ quan phải đảm bảo yêu cầu không để lộ, lọt thông tin nhà nước; phải có quy trình cụ thể và phải lưu giữ hồ sơ, biên bản thanh lý, tiêu hủy.

2. Đối với cán bộ chuyên trách Công nghệ thông tin (CNTT):

a) Tham mưu cho lãnh đạo cơ quan, đơn vị về công tác bảo đảm an toàn thông tin; vận hành an toàn các hệ thống thông tin của cơ quan, đơn vị; triển khai các biện pháp bảo đảm an toàn thông tin cho tất cả cán bộ, công chức, viên chức trong cơ quan, đơn vị mình.

b) Nắm vững và thực hiện nghiêm túc các quy định về bảo vệ bí mật Nhà Nước. Thường xuyên tự cập nhật các kiến thức về an toàn thông tin, nguy cơ tiềm ẩn có thể gây mất thông tin và các biện pháp phòng tránh khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ.

c) Thực hiện việc đánh giá, báo cáo các rủi ro gây mất an toàn thông tin và mức độ nghiêm trọng của các rủi ro đó. Các rủi ro gây mất an toàn thông tin có thể xảy ra do sự truy cập trái phép, mất, thay đổi hoặc phá hủy thông tin và hệ thống thông tin.

d) Áp dụng biện pháp quản lý và kỹ thuật phù hợp với tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin để phòng, chống nguy cơ, khắc phục sự cố an toàn thông tin.

e) Phối hợp chặt chẽ với Sở Thông tin và Truyền thông, cơ quan Công an trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn, an ninh thông tin. Tham gia các lớp tập huấn về an toàn, an ninh thông tin mạng.

3. Đối với cán bộ, công chức, viên chức và người lao động:

a) Thường xuyên cập nhật những chính sách, quy trình, thủ tục an toàn thông tin của đơn vị cũng như thực hiện những hướng dẫn về an toàn thông tin của cơ quan hoặc cán bộ chuyên trách công nghệ thông tin.

b) Hạn chế việc sử dụng chức năng chia sẻ tài nguyên, khi sử dụng chức năng này cần bật thuộc tính bảo mật bằng mật khẩu và thực hiện việc thu hồi chức năng này khi đã sử dụng xong.

c) Các tài khoản đăng nhập cần phải đặt lại mật khẩu, thay đổi mật khẩu định kỳ. Cần đăng xuất tài khoản khỏi hệ thống khi không còn sử dụng. Hoặc ngắt kết nối mạng để tránh bị các tin tặc lợi dụng, điều khiển máy tính từ xa.

d) Chỉ sử dụng Hệ thống hộp thư điện tử (mail) công vụ, hệ thống Văn phòng điện tử liên thông, cổng/trang thông tin điện tử, các hệ thống thông tin khác của cơ quan Nhà nước để gửi, nhận, đăng tải văn bản điện tử trong hoạt động của bệnh viện.

e) Sử dụng chức năng mã hóa ở mức hệ điều hành để bảo đảm các dữ liệu nhạy cảm như tài khoản, mật khẩu, các tập tin quan trọng,... được mã hóa. Các tập tin đính kèm thư điện tử, tải xuống từ Internet hoặc sao chép từ thiết bị lưu trữ cần được kiểm tra để tránh lây nhiễm các phần mềm độc hại.

Điều 6. Xây dựng và áp dụng quy trình bảo đảm an toàn thông tin

Các đơn vị phải xây dựng và áp dụng quy trình bảo đảm an toàn cho hệ thống thông tin nhằm giảm thiểu các nguy cơ gây ra sự cố, tạo điều kiện cho việc khắc phục và truy vết trong trường hợp có sự cố xảy ra.

Nội dung của quy trình bao gồm các bước cơ bản sau:

a) Lập kế hoạch bảo vệ an toàn cho hệ thống thông tin;

b) Xây dựng hệ thống bảo vệ an toàn thông tin;

c) Quản lý và vận hành hệ thống bảo vệ an toàn thông tin;

d) Kiểm tra đánh giá hoạt động của hệ thống bảo vệ an toàn thông tin;

e) Bảo trì và nâng cấp hệ thống bảo vệ an toàn thông tin.

Chương III

TRÁCH NHIỆM BẢO ĐẢM AN TOÀN, AN NINH THÔNG TIN

Điều 7. Trách nhiệm của lãnh đạo bệnh viện, lãnh đạo khoa, phòng

1. Quan tâm và ưu tiên bố trí kinh phí cho việc triển khai các biện pháp bảo đảm an toàn thông tin trong hoạt động ứng dụng CNTT của cơ quan, đơn vị.

2. Xây dựng quy chế, quy trình nội bộ về bảo đảm an toàn thông tin theo quy định tại Điều 6 quy chế này và các quy định của pháp luật.

3. Khi có sự cố mất an toàn thông tin phải kịp thời chỉ đạo khắc phục ngay, ưu tiên sử dụng cán bộ kỹ thuật chuyên trách trong cơ quan, đơn vị và thông báo bằng văn bản cho Sở Thông tin và Truyền thông, Sở Y tế để biết và phối hợp xử lý.

4. Phối hợp chặt chẽ với cơ quan Công an trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin. Tạo điều kiện thuận lợi cho các cơ quan chức năng tham gia khắc phục sự cố và thực hiện đúng theo hướng dẫn.

5. Báo cáo tình hình và kết quả thực hiện công tác bảo đảm an toàn thông tin tại đơn vị và gửi Sở Thông tin và Truyền thông, Sở Y tế khi có yêu cầu.

Điều 8. Trách nhiệm của Phòng Kế hoạch tổng hợp, Tổ IT

1. Tham mưu giúp Giám đốc bệnh viện trong công tác quản lý về đảm bảo an toàn thông tin trong cơ quan.

2. Tổ chức kiểm tra định kỳ hoặc đột xuất khi phát hiện có dấu hiệu, hành vi vi phạm an toàn thông tin, xử lý nghiêm các hành vi vi phàm an toàn thông tin theo quy định của pháp luật.

3. Hướng dẫn các tiêu chí và quy trình kỹ thuật nhằm đảm bảo an toàn thông tin; kiểm tra công tác đảm bảo an toàn thông tin; tham gia các chương trình đào tạo, bồi dưỡng và tuyên truyền về an toàn thông tin.

4. Hướng dẫn các khoa, phòng, đơn vị thực hiện các báo cáo về sự cố mất an toàn thông tin và kết quả thực hiện công tác đảm bảo an toàn thông tin.

5. Tùy theo mức độ sự cố, phối hợp các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố mất an toàn thông tin.

6. Đưa nội dung đảm bảo an toàn thông tin vào Kế hoạch ứng dụng công nghệ thông tin hàng năm của đơn vị; dự toán kinh phí để triển khai công tác đào tạo, hướng dẫn đảm bảo an toàn, an ninh thông tin cho các hệ thống thông tin của bệnh viện.

Điều 9. Trách nhiệm của cán bộ, công chức, viên chức, người lao động

1. Nghiêm chỉnh chấp hành các quy chế nội bộ, quy trình về an toàn thông tin của cơ quan cũng như quy định khác của pháp luật, nâng cao ý thức cảnh giác và trách nhiệm bảo đảm an toàn thông tin tại đơn vị.

2. Khi phát hiện sự cố phải báo ngay với cơ quan cấp trên và bộ phận chuyên trách công nghệ thông tin để kịp thời ngăn chặn, xử lý.

3. Có trách nhiệm bảo vệ, quản lý tài khoản được cấp tạm thời (nếu có) để đăng nhập vào các hệ thống thông tin thực hiện giao dịch với các cơ quan qua các dịch vụ công trực tuyến, hệ thống mail công vụ, hệ thống Văn phòng điện tử liên thông, không giao tài khoản cho người khác sử dụng.

Chương IV

KHEN THƯỞNG, KỶ LUẬT

Điều 10. Các khoa, phòng , đơn vị, cá nhân trực thuộc Bệnh viện Mắt phải chấp hành nghiêm Quy chế này. Nếu vi phạm thì tùy theo tính chất, mức độ sẽ bị xử lý, kỷ luật theo quy định.

Điều 11. Các phòng chuyên môn, đơn vị, các nhân thực hiện tốt Quy chế này được xét thi đua khen thưởng hàng năm. Người có công phát hiện, ngăn chặn kịp thời các hành vi vi phạm sẽ được khen thưởng theo Quy chế thi đua khen thưởng của bệnh viện.

Chương V

TỔ CHỨC THỰC HIỆN

Điều 12. Quy chế này được phổ biến đến tất cả công chức, viên chức, người lao động trong cơ quan. Trong quá trình thực hiện, nếu có khó khăn, vướng mắc cần điều chỉnh, sửa đổi, bổ sung; các đơn vị phản ảnh về Phòng Kế hoạch tổng hợp để tổng hợp trình Lãnh đạo bệnh viện xem xét, sửa đổi, bổ sung cho phù hợp./.

GIÁM ĐỐC

SỞ Y TẾ TỈNH BÌNH ĐỊNH
BỆNH VIỆN MẮT

Nguyễn Thanh Triết