SỞ Y TẾ QUẢNG BÌNH **BỆNH VIỆN ĐKKV BẮC QUẢNG BÌNH**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 205 /QĐ-BV	*Ba Đồn, ngày 14 tháng 3 năm 2025*

QUYẾT ĐỊNH

V/v Ban hành Quy chế đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của Bệnh viện ĐKKV Bắc Quảng Bình

GIÁM ĐỐC BỆNH VIỆN ĐA KHOA KHU VỰC BẮC QUẢNG BÌNH

Căn cứ Luật Công nghệ thông tin ngày 29 tháng 06 năm 2006;

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

Căn cứ Luật An ninh mạng ngày 12 tháng 06 năm 2018;

Căn cứ Luật Giao dịch điện tử ngày 22 tháng 6 năm 2023;

Căn cứ Luật Viễn thông ngày 24 tháng 11 năm 2023;

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10 tháng 04 năm 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 tháng 7 năm 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 tháng 7 năm 2016 của Chính phủ về đảm bảo an toàn hệ thống thông tin theo cấp độ;

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

Căn cứ Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng;

Căn cứ Nghị định số 69/2024/NĐ-CP ngày 25 tháng 6 năm 2024 của Chính phủ Quy định về định danh và xác thực điện tử;

Căn cứ Nghị định số 137/2024/NĐ-CP ngày 23 tháng 10 năm 2024 của Chính phủ Quy định về giao dịch điện tử của cơ quan nhà nước và hệ thống thông tin phục vụ giao dịch điện tử;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo

đảm an toàn thông tin mạng quốc gia;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của 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 Thông tư số 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;

Căn cứ Quyết định số 1462/QĐ-UBND ngày 08/6/2023 của UBND tỉnh Quảng Bình về việc quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bệnh viện ĐKKV Bắc Quảng Bình;

Căn cứ Quyết định số 13/2020/QĐ-UBND ngày 14/7/2020 của UBND tỉnh Quảng Bình ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước tỉnh Quảng Bình;

Xét đề nghị của Trưởng phòng Kế hoạch - Tổng hợp,

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 Bệnh viện đa khoa khu vực Bắc Quảng Bình.

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

Điều 3. Trưởng các khoa, phòng và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
-Sở Y tế (B/c);
- Như điều 3;
- Lưu: VT.

GIÁM ĐỐC

SỞ Y TẾ TỈNH QUẢNG BÌNH
BỆNH VIỆN ĐA KHOA KHU VỰC BẮC QUẢNG BÌNH

Nguyễn Viết Thái

SỞ Y TẾ QUẢNG BÌNH BỆNH VIỆN ĐKKV BẮC QUẢNG BÌNH	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc

QUY CHẾ

Đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của Bệnh viện ĐKKV Bắc Quảng Bình

(Ban hành kèm theo Quyết định số /QĐ-BV ngày / /2025 của Bệnh viện ĐKKV Bắc Quảng Bình)

Chương I

QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định các chính sách quản lý và các biện pháp nhằm bảo đảm an toàn thông tin, an ninh mạng trong hoạt động ứng dụng công nghệ thông tin của Bệnh viện đa khoa khu vực Bắc Quảng Bình (gọi tắt là các Hệ thống thông tin).

Điều 2. Đối tượng áp dụng

Các cán bộ, công chức, viên chức, người lao động của Bệnh viện đa khoa khu vực Bắc Quảng Bình.

Các khoa, phòng và các bộ phận trực thuộc, cá nhân có kết nối, sử dụng các Hệ thống thông tin.

Các tổ chức, cá nhân cung cấp dịch vụ công nghệ thông tin và an toàn thông tin mạng phục vụ hoạt động các Hệ thống thông tin.

Điều 3. Giải thích từ ngữ

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

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.

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.

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.

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.

Mạng ngang hàng là mô hình mạng mà trong đó các máy tính có quyền bình đẳng như nhau, mỗi máy tính có quyền chia sẻ tài nguyên và sử dụng các tài nguyên từ máy tính khác.

Cán bộ chuyên trách hệ thống thông tin là viên chức, người lao động được giao phụ trách an toàn thông tin/công nghệ thông tin tại cơ quan, đơn vị.

Điều 4. Mục tiêu, nguyên tắc bảo đảm an toàn thông tin

1. Mục tiêu bảo đảm an toàn thông tin

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 các Hệ thống thông tin.

2. Nguyên tắc

Các khoa, phòng, viên chức và người lao động có trách nhiệm bảo đảm an toàn thông tin mạng. Hoạt động an toàn thông tin mạng của các khoa, phòng, các tổ chức đoàn thể, các cá nhân phải đúng quy định của pháp luật, hướng dẫn của cơ quan, đơn vị có thẩm quyền và các qui định tại Quy chế này.

Các khoa, phòng, các tổ chức đoàn thể, các cá nhân không được xâm phạm an toàn thông tin mạng của tổ chức, cá nhân khác.

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.

Bảo đảm an toàn thông tin, an ninh mạng được thực hiện xuyên suốt, toàn trình trong khâu mua sắm, nâng cấp, vận hành, bảo trì và ngừng sử dụng hạ tầng, hệ thống thông tin, phần mềm, dữ liệu.

Trách nhiệm bảo đảm an toàn thông tin mạng và an ninh mạng gắn với trách nhiệm của người đứng đầu các khoa, phòng và tương đương và cá nhân trực tiếp liên quan.

Điều 5. Những hành vi nghiêm cấm

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

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; 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/4G, điện thoại di động, máy tính bảng, máy tính xách tay).

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.

Chương II

QUY ĐỊNH ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 6. 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

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;

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

Phải 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.

Khi sửa chữa, khắc phục các sự cố của máy tính dùng soạn thảo văn bản mật, các phòng chuyên môn 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.

2. Trước khi thanh lý các máy tính trong các cơ quan nhà nước, cán bộ chuyên trách công nghệ thông tin phải dùng các biện pháp kỹ thuật xoá bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính.

Điều 7. Quy định về quản lý các tài khoản truy cập vào hệ thống thông tin

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 sử dụng tài khoản truy cập với định danh duy nhất gắn với người dùng đó. Trường hợp sử dụng tài khoản dùng chung của đơn vị, phải xác định các cá nhân 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.

Cán bộ chuyên trách thực hiện quản lý tài khoản cá nhân (nếu có). Hướng dẫn 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 hệ thống thông tin 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 !, @, #, $, %,...).

Điều 8. Bảo đảm an toàn hạ tầng mạng

1. Quản lý hạ tầng mạng nội bộ

Thiết bị CNTT được trang bị tại các khoa, phòng là tài sản của Nhà nước, được quản lý, sử dụng theo quy định của Nhà nước. Các khoa, phòng, viên chức và người lao động có trách nhiệm quản lý trang thiết bị được giao.

Các thiết bị đầu cuối phải được quản lý khi kết nối vào hệ thống mạng theo địa chỉ MAC, IP. Thông tin về thiết bị đầu cuối (tên, chủng loại, địa chỉ MAC, địa chỉ IP) phải được quản lý và cập nhật

Giao phòng Kế hoạch - Tổng hợp làm công tác quản trị mạng, trực tiếp quản lý kỹ thuật và duy trì hoạt động của hệ thống thông tin của đơn vị; là đầu mối kết nối mạng LAN, mạng Internet, mạng dữ liệu chuyên dùng cho các phòng; kiểm tra hiện trạng, đề xuất sửa chữa hoặc mua mới các chủng loại thiết bị CNTT phù hợp, an toàn, bảo mật theo quy định về quản lý, sử dụng tài sản cơ quan. Thiết lập, cấu hình đầy đủ các tính năng của thiết bị mạng. Thường xuyên, kiểm tra phiên bản hệ điều hành của thiết bị mạng để cập nhật, vá lỗi khi cần thiết. Sử dụng các công cụ để dò tìm và phát hiện kịp thời các điểm yếu, lỗ hổng bảo mật và các truy cập bất hợp pháp vào hệ thống mạng. Thường xuyên kiểm tra, phát hiện những kết nối, trang thiết bị, phần mềm cài đặt bất hợp pháp vào mạng.

Giao phòng Kế hoạch - Tổng hợp đề xuất xây dựng hệ thống quản lý Hệ thống tin trong đó phải có sơ đồ logic và vật lý về hệ thống mạng, tổ chức quản lý định danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý hệ thống chặt chẽ, bảo đảm an toàn và bảo mật. Sử dụng thiết bị tường lửa, thiết bị phát hiện và kiểm soát truy cập từ bên ngoài mạng và phân chia hệ thống mạng thành các vùng mạng quản lý theo chính sách an toàn thông tin riêng; Kiểm soát truy cập từ bên trong mạng; Kết nối về hệ thống giám sát tập trung; Phòng chống xâm nhập giữa các vùng mạng; Phòng chống phần mềm độc hại trên môi trường mạng.

2. Quản lý hệ thống mạng không dây

Phối hợp với cơ quan, đơn vị cung cấp dịch vụ mạng, khi thiết lập mạng

không dây để kết nối với mạng cục bộ thông qua các điểm truy nhập (Access Point - AP), cán bộ phụ trách hệ thống thông tin phải thiết lập các tham số: Tên, nhận dạng dịch vụ (Service Set Identitìer - SSID), mật khẩu 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: !, @, #, $, %), cấp phép truy nhập đối với địa chỉ vật lý (MAC Address), mã hóa dữ liệu theo cơ chế bảo mật WPA2 hoặc WPA3;

Mật khẩu đăng nhập phải được thiết lập có độ phức tạp cao, định kỳ 6 tháng thay đổi mật khẩu nhằm tăng cường công tác bảo mật.

Điều 9. Bảo đảm an toàn dữ liệu

1. Quản lý tài khoản và chữ ký số

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 để đăng nhập vào hệ thống thông tin, cơ sở dữ liệu;

Tài khoản thư điện tử, chữ ký số chuyên dùng (xxx@quangbinh.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;

Tài khoản quản trị hệ thống được giao cho cán bộ chuyên trách công nghệ thông tin phục vụ cho công tác quản trị, phân quyền, cấu hình hệ thống đó. Viên chức quản trị hệ thống không sử dụng cùng một mật khẩu cho nhiều tài khoản khác nhau;

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, đơn vị quản lý cá nhân đó phải thông báo cho cơ quan, đơn vị vận hành để điều chỉnh, thu hồi, hủy bỏ tài khoản, chữ ký số, chứng thư số, và các tài khoản có liên quan khác đến hoạt động công vụ.

2. Khi thực hiện chia sẻ tài nguyên trên máy tính, các phòng chuyên môn, viên chức và người lao động 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.

3. Máy tính và thiết bị lưu trữ khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài cơ quan phải tháo rời bộ phận lưu trữ khỏi thiết bị và để lại cơ quan 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.

4. 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.

5. Có phương án sao lưu và khôi phục dữ liệu, dữ liệu sao lưu phải được lưu trữ an toàn và được kiểm tra thường xuyên đảm bảo sẵn sàng cho việc sử dụng khi cần kiểm tra, phục hồi hệ thống từ dữ liệu sao lưu.

Chương III

QUẢN LÝ VÀ SỬ DỤNG MẠNG, MÁY TÍNH NỘI BỘ

Điều 10. Thông tin, dich vụ và trao đổi thông tin trên mạng nội bộ

1. Các loại thông tin trên mạng:

Thông tin được cung cấp từ Internet.

Thông tin từ website Bệnh viện.

Thông tin trao đổi giữa các Khoa phòng, giữa Bệnh viện với các tổ chức khác.

2. Các dịch vụ trên mạng nội bộ:

Các dịch vụ được cung cấp từ mạng Internet: thư điện tử, tìm kiếm thông tin trên các trang Web.

Các dịch vụ được cung cấp từ các hệ thống phần mềm, các cơ sở dữ liệu phục vụ công tác quản lý điều hành của Bệnh viện hoạt động trên mạng.

Các dịch vụ được cung cấp từ các công cụ an ninh bảo mật.

Các dịch vụ chia sẽ tài nguyên mạng.

3. Trao đổi thông tin trên mạng nội bộ:

Việc trao đổi thông tin trên mạng nội bộ phải tuân thủ các quy định hiện hành của nhà nước.

Các thông tin và dịch vụ bị cấm đưa lên mạng nội bộ:

+ Thông tin của các tổ chức chính quyền, đoàn thể, các cơ quan chức năng được yêu cầu giữ bí mật.

+ Thông tin cá nhân như: tài sản cá nhân, đời tư; thông tin vi phạm quyền sở hữu trí tuệ.

+ Thông tin làm ảnh hưởng đến an ninh quốc gia;

+ Thông tin xuyên tạc, tuyên truyền chống đối các chủ trương chính sách của Đảng và Nhà nước, phá hoại khối đại đoàn kết dân tộc;

+ Những thông tin có nội dung kích động bạo lực, truyền bá tư tưởng phản động;

+ Thông tin trái với thuần phong mỹ tục như, thông tin có nội dung không lành mạnh;

+ Thông tin quấy rối cá nhân, xúc phạm danh dự, vu khống, xúc phạm đến nhân phẩm công dân;

+ Những thông tin và các ứng dụng có tính chất phá hoại như phát tán virus máy tính, lấy cắp thông tin, phá hoại cơ sở dữ liệu, làm tê liệt mạng máy tính.

+ Thông tin có ảnh hưởng xấu đến văn hoá xã hội: xuyên tạc lịch sử, phủ nhận các thành quả cách mạng, xúc phạm các vĩ nhân và các anh hùng dân tộc, phao tin đồn nhảm ảnh hưởng đến uy tín của Quốc gia;

+ Thông tin và các dịch vụ không được phép sử dụng theo quy định hiện hành của pháp luật.

Điều 11. Bảo đảm an ninh và bảo mật mạng nội bộ

Mạng nội bộ Bệnh viện phải được trang bị hệ thống kỹ thuật để quản lý, giám sát, kiểm soát mạng, nhằm phát hiện ngăn chặn các truy cập trái phép của người sử dụng, tin tặc tấn công mạng.

Người sử dụng phải đăng ký và được cung cấp thông tin về tên, mật khẩu truy cập mạng theo quy định và tuân thủ các quy định về kết nối an toàn mạng, phải thường xuyên thay đổi mật khẩu đăng nhập để đảm bảo an toàn và bảo mật dữ liệu trên mạng nội bộ.

Người sử dụng khi truy cập, sử dụng tài nguyên nội bộ, truy cập mạng và tài nguyên trên Internet phải tuân thủ các quy định của pháp luật về bảo đảm an toàn thông tin và các quy định của Bệnh viện đa khoa khu vực Bắc Quảng Bình.

Không sử dụng các máy tính thuộc sở hữu cá nhân (máy xách tay của cá nhân, thiết bị di động thông minh) hoặc những thiết bị lưu trữ di động cá nhân vào mục đích riêng. Hạn chế tối đa việc sử dụng các thiết bị lưu trữ ngoài để sao chép, di chuyển dữ liệu.

Tất cả các máy trạm phải được trang bị phần mềm phòng chống mã độc. Các phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc khi sao chép, mở các tập tin.

Việc sử dụng các thiết bị lưu trữ ngoài như ổ cứng di động, thẻ nhớ, thiết bị lưu trữ USB,... phải thường xuyên quét mã độc trước khi đọc hoặc sao chép dữ liệu.

Khi gửi văn bản điện tử gửi qua hệ thống thư điện tử phải có định dạng theo Danh mục tiêu chuẩn kỹ thuật về ứng dụng CNTT trong cơ quan nhà nước như: (.txt),

(.doc), (.odt), (.pdf) và các định dạng khác theo quy định, không được gửi các file thực thi (.com), (.bat), (.exe)....

Các cán bộ, viên chức và người lao động phải được hướng dẫn về phòng chống mã độc, các rủi ro do mã độc gây ra; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm trên máy trạm khi chưa có sự đồng ý của người có thẩm quyền theo quy định của Bệnh viện đa khoa khu vực Bắc Quảng Bình.

Khi phát hiện ra bất kỳ dấu hiện nào liên quan đến việc bị nhiễm mã độc trên máy trạm (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu), người sử dụng phải báo trực tiếp cho bộ phận có trách nhiệm của Bệnh viện đa khoa khu vực Bắc Quảng Bình để xử lý.

Phần mềm ứng dụng trước khi được cài đặt, sử dụng phải được kiểm tra xem có phần mềm độc hại tồn tại hay không. Tất cả các tập tin, thư mục phải được quét mã độc trước khi sao chép, sử dụng.

Định kỳ hằng năm thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; Thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống.

Điều 12. Quản lý sự cố an toàn thông tin

Giao phòng Kế hoạch - Tổng hợp xây dựng phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng, ứng phó sự cố ATTT mạng.

Giao phòng Kế hoạch - Tổng hợp xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13,14 Quyết định số 05/2017/QĐ-TTg.

Giao phòng Kế hoạch - Tổng hợp xây dựng và triển khai kế hoạch ứng phó sự cố an toàn thông tin theo quy định tại Điều 16 Quyết định số 05/2017/QĐ-TTg.

Giao phòng Kế hoạch - Tổng hợp xây dựng và triển khai phương án giám sát, phát hiện và cảnh báo sự cố an toàn thông tin trong quy trình ứng cứu sự cố an toàn thông tin mạng nhằm khắc phục sự cố về ATTT;

Các khoa, phòng và các tổ chức, cá nhân liên quan tuân thủ theo Quy chế này về hướng dẫn xử lý, ứng cứu các sự cố an toàn thông tin mạng.

Chương IV

TRÁCH NHIỆM SỬ DỤNG VÀ TỔ CHỨC THỰC HIỆN

Điều 13. Bảo đảm an toàn máy tính cá nhân, bảo mật cơ sở dữ liệu và an ninh mạng

Phòng Kế hoạch - Tổng hợp có trách nhiệm cài đặt, quản lý các phần mềm hệ thống và phần mềm ứng dụng trong hệ thống mạng máy tính tại Bệnh viện; 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.

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

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.

Bảo mật hệ thống mạng và truyền tin: Mạng và đường truyền được áp dụng các chế độ bảo mật cần thiết, chống xâm nhập bất hợp pháp. Bộ phận quản trị mạng 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.

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

Phòng, chống virus: Viên chức, người lao động thuộc Bệnh viện 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 link liên kết không rõ ràng; không click vào các link, tải về các file tài liệu từ các địa chỉ thư không nắm rõ thông tin, địa chỉ người gửi.

Điều 14. Trách nhiệm của viên chức, người lao động khi tham gia sử dụng và khai thác hệ thống thông tin tại Bệnh viện

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

Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo kịp thời cho viên chức phụ trách công nghệ thông tin của Bệnh viện để kịp thời ngăn chặn và xử lý.

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

Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng do Bệnh viện tổ chức.

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...;

Không sử dụng các hộp thư điện tử miễn phí Gmail, Yahoo,... trong hoạt động công vụ nhằm bảo đảm bảo mật, an toàn thông tin trên môi trường mạng, 100% viên chức thực hiện nhiệm vụ phải sử dụng mail công vụ.

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,...) 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. Nghiêm cấm việc bán, cho mượn, giao người không có trách nhiệm sử dụng thiết bị do cá nhân tự trang bị có lưu giữ bí mật Nhà nước *(nếu có).*

Không được lợi dụng việc sử dụng 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, đồi trụy, 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 đồi trụy, phản động, các chương trình không rõ nguồn gốc, các thông tin quảng cáo hấp dẫn.

Nghiêm cấm các trò chơi trực tuyến (game online) hoặc các trò chơi khác trên hệ thống máy tính của đơn vị.

Khi sử dụng hệ thống thư điện tử (Email) không được kích chuột vào bất cứ thư điện tử, tệp đính kèm, đường link, thư rác, thư quảng cáo nào không rõ nguồn gốc và không xác định được người gửi.

Phải sử dụng họ và tên thật của mình trong các trang mạng xã hội như: Facebook, Zalo, Twitter và các trang mạng xã hội khác theo quy định.

Điều 15. Khen thưởng và xử lý vi phạm an toàn thông tin

1. Khen thưởng

1.1 Tiêu chí khen thưởng

Khoa, phòng , cá nhân có sáng kiến giúp cải thiện an toàn thông tin mạng.

Đảm bảo hệ thống hoạt động an toàn, không để xảy ra sự cố nghiêm trọng.

Phát hiện, ngăn chặn thành công các cuộc tấn công mạng hoặc lỗ hổng bảo mật.

Báo cáo kịp thời các nguy cơ an toàn thông tin giúp hạn chế thiệt hại cho đơn vị.

Đóng góp tích cực vào việc xây dựng Quy chế an toàn thông tin của đơn vị.

1.2 Hình thức khen thưởng

Thưởng tiền mặt hoặc hiện vật theo quy định tại Quy chế chi tiêu nội bộ.

Cộng điểm thi đua cho cá nhân hoặc tập thể trong đánh giá xếp loại cuối năm.

Vinh danh trong cuộc họp hoặc trên hệ thống nội bộ của cơ quan.

Các hình thức khen thưởng khác do Ban giám đốc bệnh viện qui định.

2. Xử lý vi phạm

2.1 Vi phạm nhẹ (Vô ý, không gây hậu quả nghiêm trọng)

Không tuân thủ quy trình đăng nhập, sử dụng mật khẩu yếu.

Truy cập tài nguyên không được phép nhưng chưa gây hậu quả.

Chia sẻ tài khoản, mật khẩu với người khác trái quy định.

Sử dụng phần mềm không được cấp phép trong nội bộ cơ quan.

Không thực hiện sao lưu dữ liệu theo quy định.

Hình thức xử lý:

Nhắc nhở, cảnh báo bằng văn bản.

Yêu cầu viết bản kiểm điểm và cam kết không tái phạm.

Trừ điểm thi đua, xếp loại.

2.2 Vi phạm trung bình (Gây ảnh hưởng đến hoạt động của đơn vị)

Để lộ thông tin nội bộ hoặc dữ liệu quan trọng do bất cẩn.

Sử dụng thiết bị cá nhân để truy cập vào hệ thống nội bộ mà không có sự cho phép quản trị hệ thống thông tin.

Cài đặt phần mềm lạ, có nguy cơ nhiễm mã độc vào hệ thống của đơn vị.

Không báo cáo kịp thời sự cố an toàn thông tin khi phát hiện ra.

Hình thức xử lý:

Khiển trách, cảnh cáo chính thức.

Hạn chế quyền truy cập vào hệ thống trong một khoảng thời gian.

Giảm thưởng hoặc trừ lương (nếu có quy định).

Yêu cầu tham gia khóa đào tạo về an toàn thông tin.

2.3 Vi phạm nghiêm trọng (Gây hậu quả lớn, ảnh hưởng đến dữ liệu và danh tiếng của đơn vị)

Truy cập trái phép vào hệ thống mạng hoặc dữ liệu mật của đơn vị.

Phát tán thông tin nội bộ ra bên ngoài mà không được phép.

Sử dụng hệ thống của đơn vị cho mục đích cá nhân hoặc bất hợp pháp.

Phá hoại dữ liệu, gây gián đoạn hệ thống, làm thất thoát thông tin.

Không tuân thủ quy định về bảo mật khi làm việc từ xa, gây rò rỉ dữ liệu.

Cố tình không tuân thủ các biện pháp bảo mật, làm tăng nguy cơ bị tấn công mạng.

Hình thức xử lý:

Kỷ luật nghiêm khắc: Khiển trách, giáng chức hoặc đình chỉ công tác.

Sa thải nếu hành vi vi phạm đặc biệt nghiêm trọng.

Bồi thường thiệt hại (nếu gây tổn thất tài chính cho đơn vị).

Chuyển hồ sơ cho cơ quan chức năng nếu hành vi vi phạm liên quan đến pháp luật (ví dụ: đánh cắp dữ liệu, phát tán mã độc…).

Ngoài ra tùy theo mức độ vi phạm mà cá nhân có thể bị xử lý theo qui định của pháp luật.

Xử phạt hành chính: Theo Nghị định số 15/2020/NĐ-CP (sửa đổi, bổ sung bởi Nghị định 14/2022/NĐ-CP).

Truy cứu trách nhiệm hình sự: Theo Bộ luật Hình sự năm 2015 (sửa đổi, bổ sung 2017).

3. Quy trình xử lý vi phạm về an toàn thông tin

Phát hiện vi phạm: Có thể do kiểm tra định kỳ, báo cáo từ cá nhân khác hoặc hệ thống giám sát an toàn thông tin.

Xác minh sự việc: Bộ phận an toàn thông tin hoặc IT tiến hành kiểm tra, thu thập bằng chứng.

Họp xem xét mức độ vi phạm: Xác định mức độ ảnh hưởng và hành vi của cá nhân vi phạm.

Quyết định hình thức xử lý: Tùy theo mức độ vi phạm, hình thức xử lý sẽ được áp dụng.

Thi hành quyết định xử lý: Gửi thông báo chính thức, thực hiện kỷ luật nếu cần.

Giám sát sau xử lý: Đảm bảo cá nhân/tập thể vi phạm không tái phạm.

Điều 16. Tổ chức thực hiện

Căn cứ Quy chế này, trưởng các khoa, phòng có trách nhiệm tổ chức triển khai thực hiện Quy chế này trong phạm vi quản lý của mình.

Viên chức và người lao động tại các khoa, phòng có trách nhiệm thực hiện nghiêm túc Quy chế này.

Giao Phòng Kế hoạch - Tổng hợp có trách nhiệm theo dõi, đôn đốc, kiểm tra, đánh giá việc thực hiện Quy chế.

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

Phòng Kế hoạch – Tổng hợp là bộ phận chuyên trách về ATTT cho hệ thống. Chủ trì, phối hợp với các khoa, phòng và bộ phân liên quan tiến hành kiểm tra công tác bảo đảm an toàn thông tin mạng định kỳ hằng năm hoặc theo chỉ đạo của Giám đốc Bệnh viện đa khoa khu vực Bắc Quảng Bình./.