SỞ Y TẾ TỈNH KON TUM **BỆNH VIỆN TÂM THẦN**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số:16 /QĐ-BVTT	*Kon Tum, ngày 20 tháng 02 năm 2024*

QUYẾT ĐỊNH
Về việc ban hành Quy định đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Bệnh viện Tâm thần tỉnh Kon Tum

GIÁM ĐỐC BỆNH VIỆN TÂM THẦN TỈNH KON TUM

Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19/11/2015;

Căn cứ Luật công nghệ thông tin số 67/2006/QH11 ngày 29/6/2006;

Căn cứ Nghị định số 64/2007/NĐ- CP ngày 10/04/2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan, nhà nước.

Căn cứ Công văn số 2632/SYT-KHTC ngày 28/8/2018 của Sở y tế Kon Tum về việc đảm bảo bí mật nhà nước trên không gian mạng.

Căn cứ Công văn số 99/UBND-HC ngày 13/09/2018 của UBND thành Phố Kon Tum về việc đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng CNTT;

Theo đề nghị cán bộ phụ trách công nghệ thông tin và phòng Tổ chức - Hành chính – Kế hoạch – Tài chính, Bệnh viện Tâm thần tỉnh Kon Tum;

QUYẾT ĐỊNH

Điều 1. Ban hành kèm theo quyết định này Quy định đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Bệnh viện Tâm thần tỉnh Kon Tum.

Điều 2. Quyết định có hiệu lực từ ngày ký ban hành.

Điều 3. Phòng Tổ chức - Hành chính – Kế hoạch – Tài chính, các khoa chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Lãnh đạo BVTT;
- Như điều 3;
- Lưu: VT, TCHCKHTC.

GIÁM ĐỐC

SỞ Y TẾ TỈNH KON TUM
BỆNH VIỆN TÂM THẦN

Đinh Văn Khuê

SỞ Y TẾ TỈNH KON TUM
BỆNH VIỆN TÂM THẦN

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

QUY ĐỊNH
Đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Bệnh viện Tâm thần tỉnh Kon Tum

(Ban hành kèm theo Quyết định số /QĐ-BVTTngày 20 tháng 02 năm 2024 của Giám đốc Bệnh viện Tâm thần tỉnh Kon Tum)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy định này quy định về các nội dung, biện pháp để bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin trên môi trường mạng của Bệnh viện Tâm thần tỉnh Kon Tum.

Điều 2. Đối tượng áp dụng

1. Quy định này được áp dụng đối với các khoa, phòng tại Bệnh viện Tâm thần tỉnh Kon Tum.

2. Công chức, viên chức đang làm việc tại Bệnh viện Tâm thần Kon Tum, các cá nhân, tổ chức có liên quan khi tham gia vận hành, khai thác, sử dụng hệ thống CNTT tại Bệnh viện Tâm thần tỉnh Kon Tum.

Điều 3. Giải thích từ ngữ

1. *An toàn 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. *An ninh thông tin:* Là sự bảo đảm thông tin, hệ thống thông tin được phục vụ liên tục, tránh bị gián đoạn, ngăn chặn các truy cập trái phép làm sửa đổi, phá hoại hoặc rò rỉ thông tin.

3. *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 nhập, xử lý, lưu trữ và trao đổi thông tin.

4. *Hệ thống mạng Lan:* Là hệ thống mạng nội bộ dùng để kết nối các máy tính trong một phạm vi nhỏ *(Ở đây là giữa các khoa, phòng của Bệnh viện Tâm thần tỉnh Kon Tum).* Các máy tính trong mạng LAN có thể chia sẻ tài nguyên với nhau, mà điển hình là chia sẻ tập tin, máy in, máy quét và một số thiết bị khác.

5. *Địa chỉ IP:* Là một địa chỉ đơn nhất mà những thiết bị điện tử hiện nay đang sử dụng để nhận diện và liên lạc với nhau trên mạng máy tính bằng cách sử dụng giao thức Internet.

6. *Thiết bị lưu trữ ngoài:* Là các ổ cứng di động, USB, đĩa CD, DVD,…

7. *Tường lửa (Firewall):* Là rào chắn (phần cứng, phần mềm) được lập ra nhằm kiểm soát người dùng mạng Internet truy nhập vào các thông tin không mong muốn và người dùng từ bên ngoài truy nhập trái phép thông tin trong mạng nội bộ.

8. *Môi trường mạng:* Là môi trường trong đó thông tin được cung cấp, truyền đưa, thu nhập, xử lý, lưu trữ và trao đổi thông qua cơ sở hạ tầng thông tin.

Điều 4. Nguyên tắc bảo đảm an toàn, an ninh thông tin

1. Bệnh viện Tâm thần tỉnh Kon Tum có trách nhiệm phổ biến kiến thức cơ bản về an toàn, an ninh thông tin cho cán bộ công chức, viên chức của các khoa, phòng, các đơn vị trực thuộc.

2. Cá nhân thuộc các khoa, phòng tại Bệnh viện Tâm thần tỉnh Kon Tum không được xâm phạm an toàn, an ninh thông tin của cá nhân khác (tự ý truy cập máy tính, sao chép thông tin dữ liệu cá nhân mà chưa được sự đồng ý)

3. Nghiêm cấm soạn thảo, lưu trữ, sao lưu thông tin bí mật nhà nước trên máy tính hoặc thiết bị điện tử có tính năng lưu trữ thông tin có kết nối internet.

4. Không kết nối mạng nội bộ chứa thông tin bí mật nhà nước với mạng internet và ngược lại.

5. Nghiêm cấm trao đổi thông tin bí mật nhà nước qua điện thoại, fax, hộp thư điện tử mà không có giải pháp mã hóa cơ yếu.

6. Không trao đổi thông tin bí mật nhà nước qua hộp thư điện tử cá nhân và các dịch vụ OTT (các ứng dụng và các nội dung như âm thanh, video được cung cấp trên nền tảng Internet...) trên internet.

7. Các thiết bị có nội dung lưu trữ bí mật nhà nước không sử dụng nữa phải được xử lý hoặc tiêu hủy theo đúng quy trình, quy định của nhà nước về bảo vệ bí mật nhà nước.

8. Nghiêm cấm sử dụng các thiết bị có khả năng lưu trữ để sao chép dữ liệu giữa các máy tính dùng để soạn thảo nội dung bí mật nhà nước với các máy tính hoặc thiết bị, phương tiện điện tử có kết nối internet.

9. Không sử dụng các thiết bị điện tử có nguồn gốc từ Trung Quốc để soạn thảo, lưu trữ văn bản mang nội dung bí mật nhà nước.

10. Các hoạt động ứng dụng CNTT trong cơ quan nhà nước phải tuân theo nguyên tắc bảo đảm an toàn thông tin được quy định tại Điều 42, Nghị định 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về ứng dụng CNTT trong hoạt động của cơ quan nhà nước.

Chương II
CÁC QUY ĐỊNH ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 5. Quản lý tài khoản người dùng

1. Cán bộ, viên chức phải cài đặt mật khẩu cho máy tính cá nhân của mình, có trách nhiệm bảo vệ và bảo mật tài khoản, dữ liệu của cá nhân, của phòng và của cơ quan như: Hòm thư công vụ, phần mềm Một cửa điện tử (nếu có), quản lý đối tượng hưởng bảo hiểm y tế từ ngân sách Nhà nước,…; không tự ý xâm nhập các tài khoản của người khác để sử dụng; không cung cấp thông tin tài khoản của cá nhân, cơ quan cho các tổ chức, cá nhân không có liên quan.

2. Mật khẩu phải thay đổi thường xuyên hoặc định kỳ mỗi tháng 01 lần; không dùng một mật khẩu trong nhiều tài khoản.

Điều 6. Về quản lý, sử dụng cơ sở vật chất

1. Đối với các thiết bị CNTT:

a) Máy chủ phải có xác thực bằng cơ chế mật khẩu khi tự động truy cập

b) Không truy cập vào các kết nối internet không an toàn (hạn chế truy cập các trang web không rõ nội dung và không phải địa chỉ là https:\\, không có ký hiệu khóa bảo mật…)

c) Máy chủ chứa dữ liệu quan trọng và thường xuyên kết nối Internet phải cài đặt các phần mềm diệt virus có bản quyền; có cơ chế bảo vệ thư mục và tập tin khi chia sẻ tài nguyên dùng chung.

d) Cán bộ, viên chức của Bệnh viện Tâm thần có trách nhiệm quản lý trang thiết bị CNTT (máy tính, máy in, thiết bị ngoại vi..) được giao tại phòng làm việc của mình, tự quản lý dữ liệu, thông tin trên máy nếu có sự cố hoặc hỏng, lỗi báo ngay cho cán bộ phụ trách CNTT của trung tâm khắc phục, sửa chữa.

e) Máy tính và các thiết bị CNTT để nơi an toàn, tránh ảnh hưởng của các tác nhân bên ngoài như nắng, mưa…; không để các tài liệu, vật liệu dễ cháy gần máy tính và các thiết bị CNTT để tránh xảy ra cháy nổ; thường xuyên vệ sinh cho máy vi tính; hàng ngày kiểm tra theo dõi sự hoạt động của máy vi tính và các thiết bị... Khi không sử dụng nên tắt máy vi tính và các thiết bị nhằm tiết kiệm điện và phòng chống các xâm nhập trái phép.

f) Trong quá trình sử dụng các thiết bị CNTT, khi có sự cố xảy ra đối với các thiết bị CNTT của cán bộ, viên chức thì người trực tiếp sử dụng thiết bị CNTT thông báo với cán bộ phụ trách CNTT của cơ quan, đơn vị; nếu sự cố nhỏ, không phải thay thế hoặc sửa chữa linh kiện thì cán bộ được giao phụ trách CNTT của trung tâm xử lý trực tiếp. Nếu có sự cố lớn, cần phải thay thế linh kiện để sửa chữa thì người dùng thiết bị CNTT phải làm đề xuất trình lên ban lãnh đạo của trung tâm để gọi dịch vụ sửa chữa.

2. Hệ thống mạng LAN

a) Cán bộ, viên chức của Bệnh viện khi tham gia vào mạng LAN không được tự ý thay đổi các tham số mạng, nếu tự ý thay đổi tham số mạng thì người

thay đổi phải chịu hoàn toàn trách nhiệm. Trường hợp cần thiết phải thay đổi tham số mạng, báo cán bộ phụ trách công nghệ thông tin của cơ quan biết để xử lý.

b) Cán bộ phụ trách công nghệ thông tin chịu trách nhiệm kiểm tra, theo dõi, đánh giá sự hoạt động của các thiết bị mạng và các thiết bị khác theo đúng tiêu chuẩn kỹ thuật; thực hiện công tác bảo trì, bảo dưỡng định kỳ, đột xuất, giảm tối đa các sự cố kỹ thuật;

c) Cán bộ phụ trách công nghệ thông tin chịu trách nhiệm hướng dẫn, cài đặt hệ thống an ninh mạng theo đúng tiêu chuẩn an toàn bảo mật; thường xuyên kiểm tra, quét virus cho tất cả các máy tính, xử lý khắc phục kịp thời khi xảy ra sự cố, đảm bảo hệ thống mạng máy tính hoạt động ổn định, liên tục.

Điều 7. Cơ chế sao lưu dữ liệu

1. Phân loại dữ liệu sao lưu

a) Dữ liệu hệ thống

b) Các dữ liệu khác cài đặt trên máy tính cá nhân do các cán bộ, viên chức, thuộc đơn vị soạn thảo, tạo lập trên các máy tính trong mạng nội bộ.

2. Quy định thiết bị sao lưu

a) Đối với dữ liệu hệ thống: Sử dụng chức năng sao lưu dự phòng của các ứng dụng.

b) Đối với các dữ liệu khác: Các dữ liệu cần lưu trữ, các khoa, phòng và các đơn vị trực thuộc tự sao chép vào các thiết bị lưu trữ để đảm bảo dữ liệu ít nhất lưu trữ ở hai nơi đề phòng ổ đĩa cứng của máy tính bị hỏng.

3. Định kỳ sao lưu

Tùy vào mức độ quy định thời hạn mỗi loại thông tin, dữ liệu cần sao lưu.

a) Đối với dữ liệu hệ thống: Sao lưu định kỳ: 3 tháng/lần;

b) Đối với các hệ thống thông tin: Sao lưu thường xuyên;

c) Đối với các dữ liệu khác: Sao lưu khi có thay đổi thông tin.

Điều 8. Giải quyết và khắc phục sự cố về an toàn, an ninh thông tin

1. Đối với cán bộ, viên chức

a) Thông báo kịp thời cho cán bộ phụ trách CNTT của cơ quan, đơn vị khi phát hiện các sự cố gây mất an toàn, an ninh thông tin trong hệ thống mạng.

b) Trường hợp xảy ra sự cố nghiêm trọng mà cán bộ CNTT của Bệnh viện không khắc phục được phải kịp thời báo cáo cho lãnh đạo để ban lãnh đạo kịp thời báo cáo cho cơ quan chuyên môn, cán bộ phụ trách CNTT của cơ quan quản lý cấp cao hơn để có giải pháp xử lý kịp thời.

2. Đối với cán bộ phụ trách công nghệ thông tin

a) Quản lý việc di chuyển các trang thiết bị CNTT (thiết bị mạng, thiết bị ngoại vi...) của cơ quan, đơn vị.

b) Hướng dẫn người dùng các biện pháp kỹ thuật giải quyết và khắc phục sự cố; trong trường hợp sự cố xảy ra ngoài khả năng giải quyết, kịp thời báo cáo với lãnh đạo cơ quan, đơn vị; đồng thời phối hợp với cơ quan chuyên môn để cùng phối hợp khắc phục.

c) Xử lý khẩn cấp: Khi phát hiện hệ thống bị tấn công, thông qua các dấu hiệu khác thường như: Hệ thống máy tính hoạt động chậm khác thường, nội dung bị thay đổi… cần thực hiện các bước sau:

- Ngắt kết nối máy vi tính ra khỏi mạng LAN, Internet.

- Sao chép toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ ngoài (USB, ổ cứng di động,…)

- Khôi phục hệ thống bằng cách chuyển dữ liệu backup (sao lưu) mới nhất để hệ thống hoạt động ổn định.

Điều 9. Các hành vi bị nghiêm cấm

1. Cài đặt thêm các chương trình, phần mềm, can thiệp vào phần cứng và phầm mềm cài đặt sẵn, tự ý dịch chuyển, tháo lắp các trang thiết bị mà không có sự đồng ý của cấp có thẩm quyền;

2. Xâm nhập, sửa đổi, xóa bỏ nội dung thông tin của cơ quan, cá nhân khác.

3. Cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin.

4. Ngăn chặn việc truy nhập đến thông tin của cơ quan, cá nhân khác trên môi trường mạng, trừ trường hợp pháp luật cho phép.

5. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của cơ quan, cá nhân khác trên môi trường mạng.

6. Hành vi khác làm mất an toàn, bí mật thông tin của cơ quan, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 10. Trách nhiệm của ban lãnh đạo Bệnh viện Tâm thần tỉnh Kon Tum

1. Phân công cán bộ phụ trách CNTT đảm bảo, an toàn thông tin cho hệ thống thông tin.

2. Quan tâm đầu tư các thiết bị phần cứng, phần mềm liên quan đến công tác đảm bảo an toàn, an ninh thông tin.

3. Khi có sự cố hoặc nguy cơ mất an toàn, an ninh thông tin kịp thời chỉ đạo các , khoa, phòng , các trạm y tế trực thuộc và cán bộ phụ trách CNTT phối hợp chặt chẽ với các cơ quan, đơn vị phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn, an ninh thông tin.

Điều 11. Trách nhiệm của cán bộ phụ trách CNTT

1. Xây dựng kế hoạch ứng dụng CNTT hàng năm của cơ quan, đơn vị.

2. Kịp thời tham mưu, triển khai cho trung tâm những quy định, công văn hướng dẫn có liên quan đến công tác đảm bảo anh toàn, an ninh thông tin do cơ quan chuyên môn hướng dẫn.

3. Đảm bảo an toàn, an ninh thông tin đối với các máy tính, hệ thống mạng của trung tâm, các khoa, phòng và đơn vị trực thuộc.

4. Thực hiện cấp phát, thu hồi, cập nhật và quản lý tất cả các tài khoản truy cập vào hệ thống thông tin của trung tâm; hướng dẫn người dùng thay đổi mật khẩu cá nhân theo quy định.

5. Vận hành an toàn hệ thống thông tin của cơ quan, đơn vị, triển khai các biện pháp đảm bảo an toàn, an ninh thông tin cho tất cả cán bộ, công chức, viên chức trong đơn vị mình.

6. Quản lý, theo dõi các hoạt động thường xuyên và định kỳ như vận hành, sửa chữa hệ thống mạng nội bộ, các thiết bị khác…

7. Thường xuyên hướng dẫn cán bộ, viên chức khai thác và sử dụng tài nguyên CNTT và đảm bảo an toàn, an ninh thông tin

Điều 12. Đối với cán bộ, công chức, viên chức và người lao động

1. Các máy tính khi không sử dụng trong thời gian dài cần tắt máy, để tránh bị các hacker lợi dụng, sử dụng chức năng điều khiển từ xa tấn công vào hệ thống thông tin của cơ quan, đơn vị.

2. Cán bộ, viên chức tự quản lý các thiết bị công nghệ thông tin được giao sử dụng; không tự ý thay đổi và tháo lắp các thiết bị trên máy tính khi chưa có sự đồng ý của cán bộ phụ trách công nghệ thông tin; không tự ý liên hệ với cá nhân bên ngoài vào can thiệp các thiết bị và mạng máy tính.

3. Sử dụng chức năng mã hóa, đặt mật khẩu đảm bảo các dữ liệu nhạy cảm như tài khoản, mật khẩu, các tập tin văn bản,... trước khi truyền trên môi trường mạng. Các tập tin gửi đính kèm bởi thư điện tử hoặc được tải xuống từ Internet hay các thiết bị lưu trữ gắn vào hệ thống cần được kiểm tra để phòng chống lây nhiễm virus hoặc phần mềm gián điệp làm mất thông tin.

4. Không được truy cập hoặc tải thông tin từ các website độc hại, không được cài đặt các chương trình không rõ nguồn gốc…

5. Không dùng hòm thư công vụ của cá nhân và của cơ quan, đơn vị vào mục đích cá nhân như đăng ký tài khoản mạng xã hội, đăng ký mua sắm qua mạng...

6. Nghiêm chỉnh chấp hành các quy định nội bộ về an toàn, an ninh thông tin của cơ quan và các quy định khác của pháp luật; nâng cao ý thức cảnh giác và trách nhiệm, đảm bảo an toàn, an ninh thông tin tại cơ quan.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 13. Trách nhiệm thực hiện

1. Cán bộ phụ trách CNTT chịu trách nhiệm theo dõi, đôn đốc các bộ phận trực thuộc Bệnh viện Tâm thần Kon Tum thực hiện quy định này.

2. Trong quá trình thực hiện nếu có vấn đề phát sinh, vướng mắc, cán bộ, viên chức của các khoa, phòng thuộc Bệnh viện Tâm thần tỉnh Kon Tum kịp thời báo cáo về phòng Tổ chức - Hành chính – Kế hoạch – Tài chính để cán bộ phụ trách công nghệ thông tin xem xét, sửa đổi và bổ sung./.