

Số: /QĐ-BVTT

Kon Tum, ngày tháng 10 năm 2024

## QUYẾT ĐỊNH

### Về việc ban hành Quy chế bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ Bệnh viện Tâm thần

#### GIÁM ĐỐC BỆNH VIỆN TÂM THẦN

Căn cứ Quyết định số 115/QĐ-UBND ngày 06 tháng 4 năm 2023 của Ủy ban nhân dân tỉnh Kon Tum về việc thành lập Bệnh viện Tâm thần Sở Y tế tỉnh Kon Tum;

Căn cứ Quyết định số 34/2024/UBND ngày 09/6/2024 của Chủ tịch Ủy ban nhân dân tỉnh về việc ban hành Quy định phân cấp quản lý tổ chức bộ máy và cán bộ, công chức, viên chức trên địa bàn tỉnh Kon Tum;

Căn cứ Luật An ninh mạng số 24/2018/QH14 ngày 12/6/2018;

Căn cứ Nghị định 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;

Xét đề nghị của Trưởng phòng Tổ chức - Hành chính – Kế hoạch – Tài chính,

#### QUYẾT ĐỊNH:

**Điều 1.** Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ Bệnh viện Tâm thần.

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

**Điều 3.** Trưởng các khoa, phòng, viên chức và người lao động thuộc Bệnh viện Tâm thần chịu trách nhiệm thi hành quyết định này./.

#### Nơi nhận:

- Như Điều 3;
- Lãnh đạo BV;
- SYT (B/c);
- Lưu: VT, TCHCKHTC.

GIÁM ĐỐC

Đinh Văn Khuê

## QUY CHẾ

### **Bảo đảm an toàn, an ninh mạng** **Hệ thống mạng nội bộ Bệnh viện Tâm thần**

(Ban hành kèm theo Quyết định số /QĐ-BVTT

ngày tháng năm 2024 của Giám đốc Bệnh viện Tâm thần)

### Chương I:

### QUY ĐỊNH CHUNG

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

##### 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 cho Hệ thống mạng nội bộ của Bệnh viện Tâm thần:

- Phạm vi quản lý về vật lý và logic của tổ chức
- Các ứng dụng, dịch vụ hệ thống cung cấp;
- Nguồn nhân lực bảo đảm an toàn thông tin.

##### 2. Đối tượng áp dụng

- a) Các bộ phận thuộc Bệnh viện Tâm thần.
- b) Cơ quan, tổ chức, cá nhân có kết nối, sử dụng Hệ thống mạng nội bộ
- c) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ quản lý, vận hành, duy trì, phát triển và bảo đảm an toàn thông tin mạng phục vụ hoạt động của Hệ thống Mạng nội bộ.

#### Điều 2. Giải thích từ ngữ

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

1. *An toàn thông tin mạng*: là sự 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.

2. *Mạng*: là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua mạng viễn thông và mạng máy tính.

3. *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.

4. *Chủ quản hệ thống thông tin*: là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin.

### **Điều 3. 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 thông tin Hệ thống Mạng nội bộ

#### 2. Nguyên tắc

a) Cơ quan, tổ chức thuộc đối tượng áp dụng Quy chế này có trách nhiệm bảo đảm an toàn thông tin và hệ thống thông tin trong phạm vi xử lý công việc của mình theo quy định của pháp luật, hướng dẫn của cơ quan, đơn vị có thẩm quyền và các quy định tại Quy chế này.

b) Bảo đảm an toàn thông tin (ATTT) là yêu cầu bắt buộc, phải được thực hiện thường xuyên, liên tục trong quá trình:

i. Thu thập, tạo lập, xử lý, truyền tải, lưu trữ và sử dụng thông tin, dữ liệu.

ii. Thiết kế, thiết lập và vận hành, nâng cấp, hủy bỏ hệ thống thông tin.

c) Việc bảo đảm an toàn Hệ thống mạng nội bộ được thực hiện một cách tổng thể, đồng bộ, tập trung trong việc đầu tư các giải pháp bảo vệ, có sự dùng chung, chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư thừa, trùng lặp

### **Điều 4. 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.

### **Điều 5. Phối hợp với những cơ quan/tổ chức có thẩm quyền**

1. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin:

Bệnh viện Tâm thần giao Phòng Tổ chức - Hành chính – Kế hoạch – Tài chính là đầu mối liên hệ, phối hợp các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin phục vụ việc bảo đảm an toàn, an ninh mạng cho Hệ thống mạng nội bộ

2. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin:

a) *Đơn vị vận hành hệ thống thông tin mạng nội bộ*

- Người liên hệ: Ông Trần Quốc Thắng

+ Số điện thoại: 0349749395

+ Email: quochangbvdakglei@gmail.com

b) Cục An toàn thông tin/Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC)

- Người liên hệ/bộ phận: Phòng Ứng cứu sự cố

- Số điện thoại: 0869 100 317

- Email: [ir@vncert.vn](mailto:ir@vncert.vn)

- Báo cáo sự cố qua nền tảng điều phối, xử lý sự cố an toàn thông tin mạng quốc gia: <https://irlab.vn>

- Báo cáo sự cố qua website của VNCERT/CC: <https://vncert.vn>

## **Điều 6. Bảo đảm nguồn nhân lực**

### **1. Tuyển dụng**

Cán bộ được tuyển dụng vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng.

### **2. Trong quá trình làm việc**

a) Trách nhiệm bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống:

- Với người sử dụng:

+ Người sử dụng có trách nhiệm đảm bảo ATTT đối với từng vị trí công việc.

+ Phải được thường xuyên tổ chức quán triệt các quy định về ATTT, nhằm nâng cao nhận thức về trách nhiệm đảm bảo ATTT.

+ Phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp thiết bị.

- Với cán bộ quản lý và vận hành hệ thống

+ Cán bộ quản lý và vận hành hệ thống phải thiết lập phương pháp hạn chế truy cập mạng không dây, giám sát và điều khiển truy cập không dây, tổ chức sử dụng chứng thực và mã hóa để bảo vệ truy cập không dây tới hệ thống thông tin.

+ Cán bộ quản lý và vận hành hệ thống phải tổ chức quản lý định danh đối với tất cả người dùng tham gia sử dụng hệ thống thông tin.

b) Định kỳ hàng năm tổ chức hoặc tham gia phổ biến, tuyên truyền nâng cao

nhận thức về an toàn thông tin cho người sử dụng do đơn vị chắc năng tổ chức.

### 3. Chấm dứt thay đổi công việc

a) Cán bộ chấm dứt hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của tổ chức;

b) Bộ phận chuyên trách thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc.

## **Chương II:**

### **BẢO ĐẢM AN TOÀN THÔNG TIN TRONG QUẢN LÝ THIẾT KẾ, XÂY DỰNG HỆ THỐNG**

#### **Điều 7. Thiết kế an toàn hệ thống thông tin**

1. Bộ phận chuyên trách xây dựng tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin và thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống.

2. Bộ phận chuyên trách xây dựng tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống.

#### **Điều 8. Thử nghiệm và nghiệm thu hệ thống**

1. Bên triển khai xây dựng kế hoạch, nội dung thử nghiệm hệ thống trước khi thực hiện thử nghiệm và nghiệm thu hệ thống.

2. Đơn vị vận hành thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác theo phương án thiết kế được phê duyệt trong Hồ sơ đề xuất cấp độ.

## **Chương III:**

### **BẢO ĐẢM AN TOÀN THÔNG TIN TRONG QUẢN LÝ VẬN HÀNH HỆ THỐNG**

#### **Điều 9. Quản lý an toàn mạng**

1. Hệ thống mạng phải được thiết kế thống nhất, được quản lý định danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý và bảo đảm an toàn và bảo mật.

2. Hệ thống mạng nội bộ (LAN) phải được bảo vệ bằng tường lửa (có thể tích hợp tường lửa trên modem hoặc router) và phân chia hệ thống mạng thành các vùng mạng quản lý theo chính sách an toàn thông tin riêng.

3. Mạng không dây (WIFI), cần thiết lập các thông số an toàn và định kỳ ít nhất 03 tháng thay đổi mật khẩu truy cập nhằm tăng cường công tác bảo mật. Hệ thống mạng không dây phải được bảo vệ bởi mật khẩu an toàn.

#### **Điều 10. Quản lý an toàn máy chủ và ứng dụng**

1. Máy chủ phải được thiết lập chính sách xác thực và kiểm soát truy cập. Các hệ thống thông tin cần có phương án giới hạn số lần đăng nhập, 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.

2. Kiểm tra, giám sát các hoạt động liên quan đến các nơi lưu trữ mật khẩu và cảnh báo khi có những hành động bất thường (Ví dụ: user không có quyền nhưng cố tình truy xuất đến các file lưu mật khẩu...).

#### **Điều 11. Quản lý an toàn dữ liệu**

1. Có cơ chế sao lưu dữ liệu dự phòng, lưu trữ dữ liệu tại nơi an toàn đồng thời thường xuyên kiểm tra để đảm bảo sẵn sàng phục hồi nhằm ngăn ngừa và hạn chế khi sự cố an toàn thông tin mạng xảy ra. Dữ liệu trên máy chủ được sao lưu thông qua hệ thống sao lưu dữ liệu.

2. Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ và các thông tin, dữ liệu quan trọng khác trên hệ thống theo yêu cầu của đơn vị vận hành.

3. Quyền truy cập phải được phân ra theo từng cấp độ tương ứng với từng nhiệm vụ của nhân viên và phải được phê duyệt từ cấp trên.

#### **Điều 12. Quản lý an toàn người sử dụng đầu cuối**

Chính sách, quy trình quản lý an toàn người sử dụng đầu cuối bao gồm:

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

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

3. Các thiết bị đầu cuối khi kết nối phải được quản lý và cập nhật thông tin (tên, chủng loại, địa chỉ MAC, địa chỉ IP). Cần sử dụng cơ chế xác thực và sử dụng giao thức mạng an toàn

4. Bộ phận chuyên trách về an toàn thông tin phải thường xuyên theo dõi, kiểm tra các lỗ hổng bảo mật và quản lý kết nối, truy cập khi sử dụng thiết bị đầu cuối từ xa.

5. Bộ phận chuyên trách về an toàn thông tin thường xuyên theo dõi cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống đối với các nhân viên đã nghỉ việc.

6. Bộ phận chuyên trách về an toàn thông tin thường xuyên theo dõi cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho máy tính người sử dụng và thực hiện quy trình trước khi đưa hệ thống vào sử dụng.

### **Điều 13. Quản lý rủi ro an toàn thông tin mạng**

Đơn vị vận hành xây dựng và ban hành Hồ sơ Quản lý rủi ro an toàn thông tin bao gồm các nội dung sau:

1. Danh mục tài sản thông tin, dữ liệu có trong hệ thống.
2. Đánh giá các rủi ro an toàn thông tin đối với mỗi loại tài sản.
3. Có phương án dự phòng và khôi phục sau sự cố đối với thông tin, dữ liệu và ứng dụng.

### **Điều 14. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ**

Quy định, quy trình về Kết thúc vận hành, khai thác, thanh lý, hủy bỏ bao gồm các nội dung sau:

1. Thiết bị CNTT có chứa dữ liệu (máy tính, thiết bị lưu trữ, ...) khi bị hỏng phải được cán bộ vận hành kiểm tra, sửa chữa, khắc phục. Phải có biện pháp kiểm tra, giám sát đảm bảo không để lọt lộ thông tin hay lây nhiễm mã độc đối với máy tính mang ra bên ngoài sửa chữa, bảo hành.

2. Trước khi tiến hành thanh lý/loại bỏ thiết bị công nghệ thông tin cũ, phải áp dụng các biện pháp kỹ thuật xóa bỏ hoàn toàn dữ liệu người dùng đã tạo ra, đảm bảo không thể phục hồi.

3. Các phương tiện và thiết bị CNTT: Máy tính cá nhân (PC), máy tính xách tay, máy chủ, các thiết bị mạng, phương tiện lưu trữ như CD/DVD, thẻ nhớ, ổ cứng phải xóa sạch dữ liệu khi chuyển giao hoặc thay đổi mục đích sử dụng.

## **Chương IV:**

### **TỔ CHỨC BẢO ĐẢM AN TOÀN THÔNG TIN**

#### **Điều 15. Trách nhiệm của đơn vị**

Thực hiện trách nhiệm theo quy định tại Điều 22 Nghị định 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về về bảo đảm an toàn hệ thống thông tin theo cấp độ.

#### **Điều 16. Trách nhiệm của Phòng Tổ chức - Hành chính – Kế hoạch – Tài chính**

1. Giao Phòng Tổ chức - Hành chính – Kế hoạch – Tài chính là bộ phận chuyên trách về an toàn thông tin, có trách nhiệm bảo đảm an toàn thông tin cho hệ thống thông tin

2. Tuân thủ các quy định về trách nhiệm của bộ phận chuyên trách về an toàn thông tin được giao tại Quy chế này.

#### **Điều 17. Trách nhiệm của người dùng**

Thực hiện nghiêm túc các quy định về quản lý, vận hành hệ thống tại đơn vị theo đúng các quy định hiện hành. Chấp hành đúng các quy định về an toàn thông tin tại Điều 12 Quy chế này.

### **Chương V: TỔ CHỨC THỰC HIỆN**

#### **Điều 18. Xây dựng và công bố**

Quy chế này được tổ chức/bộ phận trình người đứng đầu đơn vị vận hành trước khi công bố áp dụng.

#### **Điều 19. Rà soát, cập nhật, bổ sung Quy chế**

1. Định kỳ 03 năm hoặc khi có thay đổi Quy chế bảo đảm an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung.

2. Có hồ sơ lưu lại thông tin phản hồi của đối tượng áp dụng chính sách trong quá trình triển khai, áp dụng chính sách an toàn thông tin.