SỞ Y TẾ TỈNH KON TUM
TRUNG TÂM Y TẾ
HUYỆN ĐĂK TÔ

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

QUY CHẾ
đảm bảo an toàn, an ninh thông tin cho Hệ thống mạng nội bộ của Trung tâm Y tế huyện Đăk Tô

(Ban hành kèm theo Quyết định số 287/QĐ-YTĐT ngày 04 tháng 10 năm 2024 của Trung tâm Y tế huyện Đăk Tô)

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 Trung tâm Y tế huyện Đăk Tô bao gồm:

- 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 khoa, phòng, trạm y tế; viên chức, người lao động (gọi tắt là viên chức) thuộc Trung tâm tế huyện Đăk Tô.

b) Cơ quan, tổ chức, cá nhân có kết nối, sử dụng Hệ thống mạng nội bộ của Trung tâm Y tế huyện Đăk Tô.

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 của Trung tâm Y tế huyện Đăk Tô.

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.

5. Hệ thống mạng nội bộ (LAN - Local Area Network): là hệ thống mạng nội bộ được thiết kế để kết nối các máy tính trong một phạm vi nhỏ.

6. Người dùng (User): là người sử dụng hạ tầng hệ thống Công nghệ thông tin.

7. Mạng không dây (Wi-Fi): là công nghệ truyền dữ liệu giữa các thiết bị qua sóng vô tuyến mà không cần dây dẫn.

8. Ký tự đặc biệt: là các ký tự !"# $%& '() *+, -./ : ;<=>?@ [\]^_` {|}~.

9. IP (Internet Protocol): Địa chỉ duy nhất dùng để xác định và định danh thiết bị trên mạng, cho phép chúng gửi và nhận dữ liệu.

10. Vùng riêng biệt (subnets): là phân đoạn của một mạng lớn, cho phép chia nhỏ địa chỉ IP thành các nhóm nhỏ hơn để quản lý, tổ chức và cải thiện hiệu suất mạng.

11. Giao thức TCP/IP: Bộ quy tắc cho phép truyền dữ liệu qua Internet, bao gồm TCP (đảm bảo dữ liệu không mất) và IP (xác định địa chỉ thiết bị).

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 của Trung tâm Y tế huyện Đăk Tô.

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:

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

- 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 của Trung tâm Y tế huyện Đăk Tô 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:

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

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

3. Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của biện pháp bảo vệ an toàn thông tin mạng của hệ thống thông tin; tấn công, chiếm quyền điều khiển, phá hoại hệ thống thông tin.

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

5. Thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác; lợi dụng sơ hở, điểm yếu của hệ thống thông tin để thu thập, khai thác thông tin cá nhân.

6. Xâm nhập trái pháp luật bí mật mật mã và thông tin đã mã hóa hợp pháp của cơ quan, tổ chức, cá nhân; tiết lộ thông tin về sản phẩm mật mã dân sự, thông tin về khách hàng sử dụng hợp pháp sản phẩm mật mã dân sự; sử dụng, kinh doanh các sản phẩm mật mã dân sự không rõ nguồn gốc.

7. Hành vi quy định tại khoản 1 Điều 18 của Luật An ninh mạng số 24/2018/QH14.

8. Tổ chức, hoạt động, câu kết, xúi giục, mua chuộc, lừa gạt, lôi kéo, đào tạo, huấn luyện người chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam.

9. Xuyên tạc lịch sử, phủ nhận thành tựu cách mạng, phá hoại khối đại đoàn kết toàn dân tộc, xúc phạm tôn giáo, phân biệt đối xử về giới, phân biệt chủng tộc.

10. Thông tin sai sự thật gây hoang mang trong Nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác.

11. Hoạt động mại dâm, tệ nạn xã hội, mua bán người; đăng tải thông tin dâm ô, đồi trụy, tội ác; phá hoại thuần phong, mỹ tục của dân tộc, đạo đức xã hội, sức khỏe của cộng đồng.

12. Xúi giục, lôi kéo, kích động người khác phạm tội.

13. Thực hiện tấn công mạng, khủng bố mạng, gián điệp mạng, tội phạm mạng; gây sự cố, tấn công, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt hoặc phá hoại hệ thống thông tin quan trọng về an ninh quốc gia.

14. Sản xuất, đưa vào sử dụng công cụ, phương tiện, phần mềm hoặc có hành vi cản trở, gây rối loạn hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; phát tán chương trình tin học gây hại cho hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; xâm nhập trái phép vào mạng viễn thông, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử của người khác.

15. Chống lại hoặc cản trở hoạt động của lực lượng bảo vệ an ninh mạng; tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng biện pháp bảo vệ an ninh mạng.

16. Lợi dụng hoặc lạm dụng hoạt động bảo vệ an ninh mạng để xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân hoặc để trục lợi.

17. Hành vi khác vi phạm quy định của Luật An ninh mạng số 24/2018/QH14.

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:

Trung tâm Y tế huyện Đăk Tô giao phòng Kế hoạch - Nghiệp vụ - Điều dưỡng - Kiểm soát nhiễm khuẩn 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 của Trung tâm Y tế huyện Đăk Tô.

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

- Tên đơn vị vận hành: Phòng Kế hoạch - Nghiệp vụ - Điều dưỡng - Kiểm soát nhiễm khuẩn.

- Quy định chức năng, nhiệm vụ và quyền hạn: Quyết định số 353/QĐ-YTĐT ngày 14/9/2022 của Trung tâm Y tế huyện Đăk Tô về quy định chức năng, nhiệm vụ các khoa, phòng và trạm y tế thuộc Trung tâm Y tế huyện Đăk Tô.

- Người đại diện: Bà Lê Thị Xuân, Chức vụ: Phó Trưởng phòng

- Địa chỉ: Khối 9, thị Trấn Đăk Tô, huyện Đăk Tô, tỉnh Kon Tum.

- Thông tin liên hệ:

+ Số điện thoại: 0963.566.058

+ Thư điện tử: bsxuan804@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

- 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.

a) Mục đích và chức năng của hệ thống: Hệ thống phục vụ công tác khám chữa bệnh; quản lý văn bản điều hành tại Trung tâm Y tế huyện Đăk Tô, hỗ trợ lưu trữ và xử lý thông tin bệnh nhân, hồ sơ y tế.

b) Đối tượng sử dụng: là các khoa, phòng, trạm y tế, viên chức, người lao động trực thuộc Trung tâm Y tế huyện Đăk Tô.

c) Phạm vi áp dụng: tại Trung tâm Y tế huyện Đăk Tô.

d) Yếu tố an toàn thông tin: bảo mật thông tin người dùng và các biện pháp bảo vệ khác.

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.

a) Kiến trúc hệ thống: Hệ thống bao gồm dịch vụ phần mềm thuê từ VNPT, máy chủ lưu trữ dữ liệu, thiết bị mạng (Router, Switch) và thiết bị đầu cuối (máy tính, máy tính bảng) kết nối qua mạng nội bộ (LAN) và Internet.

b) Giao thức truyền thông: sử dụng các giao thức TCP/IP và HTTPS để truyền tải dữ liệu.

c) Yêu cầu an toàn thông tin: Các yêu cầu kỹ thuật bảo vệ dữ liệu, như tường lửa, phần mềm chống virus và mã hóa.

d) Thành phần bảo mật: phần mềm diệt virus BKAV, tường lửa (firewall) Cisco.

e) Thuyết minh trong Hồ sơ đề xuất cấp độ: Tất cả tài liệu mô tả thiết kế và thành phần được thuyết minh rõ ràng trong Hồ sơ đề xuất cấp độ.

Điều 8. Thử nghiệm và nghiệm thu hệ thống

1. Thực hiện vận hành thử và nghiệm thu hệ thống trước khi bàn giao và đưa vào sử dụng.

2. Có nội dung, kế hoạch thực hiện vận hành thử/kiểm thử theo quy định.

3. Có bộ phận có trách nhiệm thực hiện tham gia vận hành thử/kiểm thử và nghiệm thu hệ thống.

4. Có báo cáo nghiệm thu được xác nhận của bộ phận chuyên trách và phê duyệt của chủ quản hệ thống thông tin trước khi đưa vào sử dụng.

Chương III
BẢO ĐẢM AN TOÀN THÔNG TIN TRONG QUẢN LÝ VẬN HÀNH HỆ THỐNG

Điều 9. Quản lý an toàn mạng

1. Quản lý, vận hành hoạt động bình thường của hệ thống:

a) Bảo đảm cho hệ điều hành, phần mềm cài đặt trên máy chủ hoạt động liên tục, ổn định và an toàn.

b) Thường xuyên kiểm tra cấu hình, các tệp tin nhật ký hoạt động của hệ điều hành, phần mềm nhằm kịp thời phát hiện và xử lý những sự cố nếu có.

c) Quản lý các thay đổi cấu hình kỹ thuật của hệ điều hành, phần mềm.

d) Thường xuyên cập nhật các bản vá lỗi hệ điều hành, phần mềm từ nhà cung cấp.

đ) Loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không còn nhu cầu sử dụng.

e) Các bản quyền phần mềm cần được thống kê, quản lý thời gian phục vụ cho việc gia hạn và duy trì việc gia hạn bản quyền, dịch vụ bản quyền hàng năm.

g) Triển khai hệ thống phát hiện phòng chống xâm nhập giữa các vùng mạng quan trọng.

h) Sử dụng thêm các phương pháp xác thực đa nhân tố đối với các thiết bị mạng quan trọng.

i) Duy trì 02 kết nối mạng Internet từ các nhà cung cấp dịch vụ sử dụng hạ tầng kết nối trong nước khác nhau.

2. Bảo vệ hệ thống mạng nội bộ (LAN):

a) Tường lửa (Firewall): sử dụng tưởng lửa phần cứng Cisco.

b) Phân chia mạng: chia thành các vùng riêng biệt (subnets) theo chức năng.

3. Mạng không dây (Wi-Fi):

a) Thiết lập các thông số an toàn và định kỳ ít nhất 3 tháng thay đổi mật khẩu truy cập nhằm tăng cường công tác bảo mật.

b) Sử dụng giao thức bảo mật WPA3 hoặc WPA2. Kích hoạt tính năng ẩn SSID.

Điều 10. Quản lý an toàn ứng dụng

1. Hệ thống camera giám sát:

- Giám sát các khoa nội trú tại Trung tâm 24/24.

- Bảo vệ có thể theo dõi trên điện thoại di động.

- Được ghi hình và lưu liên tục.

- Hệ thống camera giám sát phải được định kỳ bảo trì, tối thiểu một lần trong 3 tháng.

2. Truy cập ứng dụng:

a) Thay đổi các tài khoản, mật khẩu mặc định ngay khi đưa hệ điều hành, phần mềm vào sử dụng.

b) Toàn bộ máy chủ và thiết bị công nghệ thông tin không phải máy tính ngoại trừ các hệ thống bắt buộc phải có giao tiếp với Internet (các hệ thống phục vụ truy cập Internet; cung cấp giao diện ra Internet của trang tin điện tử; phục vụ cập nhật bản vá hệ điều hành, mẫu mã độc, mẫu điểm yếu, mẫu tấn công) không được kết nối Internet.

c) Sử dụng cơ chế xác thực đa nhân tố khi truy cập vào các máy chủ trong hệ thống, các tài khoản quản trị của ứng dụng; có cơ chế yêu cầu người sử dụng thay đổi thông tin xác thực định kỳ.

d) Kiểm tra tính toàn vẹn của các tệp tin hệ thống và tính toàn vẹn của các quyền đã được cấp trên các tài khoản hệ thống.

e) Sử dụng cơ chế mã hóa thông tin xác thực của người sử dụng/bên sử dụng trước khi gửi đến ứng dụng qua môi trường mạng.

f) Xác thực thông tin, nguồn gửi khi trao đổi thông tin trong quá trình quản trị ứng dụng (không phải là thông tin, dữ liệu công khai) qua môi trường mạng.

3. Quản lý mật khẩu:

a) Bộ phận Công nghệ thông tin có trách nhiệm tiếp nhận mật khẩu quản trị hệ thống sau khi hệ thống được triển khai lần đầu và bàn giao cho một cán bộ vận hành hệ thống có biên bản kèm theo.

b) Cán bộ quản trị hệ thống phải đổi mật khẩu sau khi tiếp nhận trong vòng 01 ngày và báo cáo Bộ phận Công nghệ thông tin lưu vào nơi an toàn (cho vào phong bì, để vào tủ có khóa).

c) Mật khẩu tài khoản người dùng phải được giữ bí mật và chỉ bàn giao cho đúng người đăng ký tài khoản đó.

d) Mật khẩu phải đảm bảo độ phức tạp về độ dài, nội dung và thời gian sử dụng:

- Độ dài của mật khẩu:

+ Đối với mật khẩu của người dùng (sử dụng đăng nhập hệ thống, thư điện tử, ứng dụng nghiệp vụ, Internet, máy tính cá nhân): Độ dài tối thiểu là 8 ký tự.

+ Đối với mật khẩu quản trị hệ thống (sử dụng cho việc quản trị các hệ thống mạng, bảo mật, máy chủ, thư điện tử, ứng dụng nghiệp vụ): Độ dài tối thiểu là 8 ký tự.

- Nội dung mật khẩu:

+ Nội dung của mật khẩu không bao gồm các từ dễ nhớ như tên, ngày sinh, số điện thoại.

+ Nội dung mật khẩu quản trị hệ thống phải bao gồm, kết hợp các loại sau: chữ cái in thường, chữ cái in hoa, ký tự đặc biệt, số.

- Thời gian sử dụng mật khẩu:

+ Đối với mật khẩu của người dùng: mật khẩu định kỳ phải được định kỳ thay đổi, tối thiểu một lần trong 6 tháng.

+ Đối với mật khẩu quản trị hệ thống: mật khẩu định kỳ phải được định kỳ thay đổi, tối thiểu một lần trong 3 tháng và không lặp lại trong 3 lần.

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.

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

1. Cài đặt, cập nhật, sử dụng phần mềm phòng chống mã độc; dò quét, kiểm tra phần mềm độc hại trên máy tính, máy chủ và thiết bị di động.

2. Cài đặt, sử dụng phần mềm trên máy tính, thiết bị di động và việc truy cập các trang thông tin trên mạng.

3. Gửi nhận tập tin qua môi trường mạng và các phương tiện lưu trữ di động.

4. Định kỳ hàng 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 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 xoá 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 Trung tâm Y tế huyện Đăk Tô

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, cụ thể:

1. Thường xuyên kiểm tra, rà soát việc quản trị, vận hành hệ thống thông tin của Trung tâm Y tế huyện.

2. Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền.

3. Cử đầu mối phối hợp với Sở Thông tin và Truyền thông tham gia các hoạt động bảo đảm an toàn thông tin mạng trên địa bàn tỉnh.

4. Hàng năm, đề xuất nhu cầu đào tạo, tập huấn, bồi dưỡng kiến thức về đảm bảo an toàn thông tin.

Điều 16. Trách nhiệm của Phòng Kế hoạch - Nghiệp vụ - Điều dưỡng - Kiểm soát nhiễm khuẩn

1. Giao Phòng Kế hoạch - Nghiệp vụ - Điều dưỡng - Kiểm soát nhiễm khuẩn 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

1. Chính sách được Trung tâm Y tế huyện Đăk Tô thông qua trước khi công bố áp dụng.

2. Chính sách được công bố trước khi áp dụng.

3. Tổ chức tuyên truyền, phổ biến cho toàn bộ cán bộ, viên chức và người lao động của Trung tâm Y tế huyện Đăk Tô.

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.