SỞ Y TẾ AN GIANG **TRUNG TÂM Y TẾ HÀ TIÊN**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 203/QĐ-TTYT	*Tô Châu, ngày 22 tháng 8 năm 2025*

QUYẾT ĐỊNH

Ban hành Quy định đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin tại Trung tâm Y tế Hà Tiên

GIÁM ĐỐC TRUNG TÂM Y TẾ HÀ TIÊN

Căn cứ Luật Công nghệ thông tin 27/VBHN-VPQH ngày 02/08/2023;

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

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động cơ quan Nhà nước;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định 1350/QĐ-BTTTT ngày 12/08/2024 của Bộ Thông tin và Truyền thông về việc bổ sung, thay thế một số nội dung tại quyết định số 121/QĐ-BTTTT ngày 01/02/2024 của bộ trưởng bộ thông tin và truyền thông về việc công bố kết quả hệ thống hóa văn bản quy phạm pháp luật thuộc lĩnh vực quản lý nhà nước của bộ thông tin và truyền thông kỳ 2019 - 2023;

Căn cứ Quyết định số 326/QĐ-BYT ngày 07/02/2024 của Bộ trưởng Bộ Y tế ban hành, quy định về Quy chế bảo đảm an toàn thông tin và an ninh mạng trong các hoạt động ứng dụng công nghệ thông tin của Bộ Y tế;

Căn cứ Quyết định số 531/QĐ-TTYT, ngày 11/8/2025 của Ủy ban nhân dân tỉnh An Giang về việc thành lập Trung tâm Y tế Hà Tiên;

Theo đề nghị của Trưởng Phòng Kế hoạch Nghiệp vụ,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy định đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin tại Trung tâm Y tế Hà Tiên.

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

Điều 3. Các ông (bà) Trưởng các khoa, phòng, công chức, viên chức, người lao động và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Sở Y tế (để b/c);
- Như Điều 3;
- Ban Giám đốc;
- Lưu: VT, KHNV.

GIÁM ĐỐC
PHÓ GIÁM ĐỐC

SỞ Y TẾ TỈNH AN GIANG
TRUNG TÂM Y TẾ HÀ TIÊN

Nguyễn Hiếu Nghĩa

QUY ĐỊNH
Bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng Công nghệ thông tin của Trung tâm Y tế Hà Tiên

(Kèm theo Quyết định số /QĐ-TTYT, ngày tháng 8 năm 2025 của Giám đốc Trung tâm Y tế Hà Tiên)

CHƯƠNG I
NHỮNG QUY ĐỊNH CHUNG

Điều 1. Phạm vi áp dụng

Quy định này quy định về bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của Trung tâm Y tế Hà Tiên.

Điều 2. Đối tượng áp dụng

Quy định này áp dụng đối với viên chức, người lao động trong các Khoa, Phòng trong việc quản lý, khai thác, sử dụng và đảm bảo an toàn, an ninh thông tin của Trung tâm Y tế Hà Tiên phục vụ công tác chuyên môn.

Điều 3. Giải thích từ ngữ

Trong Quy định này, các từ ngữ dưới đây được hiểu như sau:

1. An toàn thông tin mạng được quy định tại Khoản 1, Điều 3, Luật An toàn thông tin mạng.

2. Hệ thống thông tin được quy định tại Khoản 3, Điều 3, Luật An toàn thông tin mạng.

3. Hạ tầng kỹ thuật được quy định tại Khoản 7, Điều 3, Nghị định số 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước.

4. Phần mềm độc hại được quy định tại Khoản 11, Điều 3, Luật An toàn thông tin mạng.

Điều 4. Nguyên tắc bảo đảm an toàn thông tin mạng

1. Hoạt động ứng dụng công nghệ thông tin của các cơ quan phải tuân theo nguyên tắc đảm bảo an toàn thông tin được quy định tại Điều 4, Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19 tháng 11 năm 2015.

2. Đảm bảo an toàn thông tin là yêu cầu bắt buộc trong triển khai ứng dụng công nghệ thông tin phục vụ hoạt động khám, chữa bệnh, quản lý, điều hành của Trung tâm Y tế Hà Tiên bao gồm: Thu thập, tạo lập, xử lý, truyền tải, lưu trữ, sử dụng thông tin, dữ liệu; thiết kế, vận hành, nâng cấp, hủy bỏ hệ thống thông tin.

Điều 5. Các hành vi bị cấm

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

Điều 6. Tổ chức đảm bảo an toàn thông tin

1. Phòng Kế hoạch Nghiệp vụ là bộ phận chuyên trách về an toàn thông tin mạng của Trung tâm Y tế Hà Tiên; Thực hiện chức năng của bộ phận chuyên trách về An toàn thông tin mạng theo quy định của pháp luật.

2. Phòng Kế hoạch Nghiệp vụ là đơn vị chịu trách nhiệm vận hành hệ thống mạng của Trung tâm Y tế Hà Tiên; Thực thi, triển khai các biện pháp đảm bảo an toàn thông tin cho các hệ thống thông tin của Trung tâm Y tế.

Điều 7. Đảm bảo nguồn nhân lực

1. Tuyển dụng: Viên chức, người lao động được tuyển dụng hoặc sắp xếp, giao nhiệm vụ về an toàn hệ thống thông tin có trình độ chuyên ngành phù hợp yêu cầu đối với vị trí việc làm về công nghệ thông tin, an toàn thông tin theo hướng dẫn của Bộ thông tin và Truyền thông.

2. Quá trình làm việc

a) Viên chức, người lao động phải tuân thủ quy định này và các quy định khác của pháp luật có liên quan về đảm bảo an toàn thông tin mạng; tham gia đầy đủ các chương trình đào tạo nâng cao nhận thức về an toàn thông tin mạng khi được triệu tập.

b) Các thông tin tuyên truyền, phổ biến kiến thức về an toàn phải được phổ biến đến 100% viên chức, người lao động trong cơ quan trên phần mềm Quản lý văn bản và điều hành.

3. Chấm dứt hoặc thay đổi công việc

a) Viên chức, người lao động nghỉ việc hoặc thay đổi công việc phải thu hồi các tài khoản, quyền truy cập hệ thống, các thiết bị máy móc, phần cứng, phần mềm và các tài khoản khác (nếu có) thuộc sở hữu của Trung tâm Y tế Hà Tiên.

b) Trưởng các Khoa, Phòng trực thuộc có trách nhiệm phối hợp với Phòng Kế hoạch Nghiệp vụ trong việc thu hồi tài sản, tài khoản, quyền truy cập của viên chức, người lao động nghỉ việc hoặc thay đổi công việc.

CHƯƠNG II
ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN TRONG QUẢN LÝ THIẾT KẾ XÂY DỰNG HỆ THỐNG THÔNG TIN

Điều 7. Thiết kế an toàn hệ thống thông tin

1. Đơn vị được giao chủ trì xây dựng mới hệ thống thông tin có trách nhiệm phối hợp với đơn vị tư vấn triển khai xây dựng hồ sơ đề xuất cấp độ an toàn hệ thống thông tin và phương án đảm bảo an toàn thông tin theo cấp độ để triển khai đồng thời quá trình triển khai dự án theo đúng các quy định 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.

2. Khi hệ thống thông tin có thay đổi thiết kế cần đánh giá lại tính phù hợp

của phương án đảm bảo an toàn thông tin để kịp thời sửa đổi, bổ sung.

3. Trường hợp hệ thống xây dựng theo hình thức thuê khoán, trong hợp đồng thuê phải có điều kiện liên quan đến bảo đảm hệ thống thông tin theo cấp độ.

4. Đối với hệ thống thông tin cấp độ 3 trở lên phải thực hiện kiểm thử phần mềm, kiểm tra an toàn thông tin trước khi đưa vào sử dụng hoặc cấp dịch vụ Internet.

5. Tài liệu kiểm thử phần mềm, kiểm thử an toàn thông tin, thử nghiệm, nghiệm thu kỹ thuật phải được đảm bảo an toàn thông tin.

Điều 8. Thử nghiệm và nghiệm thu hệ thống

1. Khi phát triển phần mềm nội bộ, đối với các hệ thống thông tin theo yêu cầu bắt buộc phải kiểm thử theo quy định của Pháp luật, trước khi đưa vào sử dụng phải kiểm thử để đảm bảo an toàn thông tin.

2. Các hệ thống hạ tầng kỹ thuật khác phải tuân thủ vận hành thử, nghiệm thu trước khi đưa vào sử dụng, đơn vị chủ trì có trách nhiệm phối hợp với đơn vị tư vấn triển khai và các tổ chức, cá nhân liên quan tổ chức vận hành thử và nghiệm thu.

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

Điều 9. Quản lý an toàn mạng

1. Viên chức người lao động trong cơ quan khi sử dụng máy tính trong nội bộ không được tự ý thay đổi đại chỉ IP và địa chỉ default gateway đã được mặc định.

2. Không được tự ý lắp đặt thiết bị thu, phát sóng Wifi (Access Point Route Wifi) vào mạng khi chưa thống nhất với Phòng Kế hoạch Nghiệp vụ.

3. Thiết bị không dây trong mạng nội bộ phải được đặt mật khẩu truy cập, thường xuyên thay đổi; Sao lưu các tập tin cấu hình hệ thống của các thiết bị quan trọng để sẵn sàng khôi phục khi xảy ra sự cố.

4. Không cung cấp mật khẩu của các thiết bị phát sóng Wifi trong mạng nội bộ ra bên ngoài, trừ các đoàn trực tiếp đến làm việc tại Trung tâm Y tế.

5. Việc sử dụng mạng riêng ảo (VPN- Vitual Private Network) khi có nhu cầu cần làm việc từ xa, bắt buộc phải đặt mật khẩu với độ an toàn cao theo quy định của Khoản 7, điều 10 và thay đổi mật khẩu tối thiểu 03 lần/tháng.

6. Hạn chế tối đa sử dụng chức năng chia sẻ tài nguyên trên các máy tính cá nhân (sharing), trừ máy in. Trường hợp cần thiết sử dụng chức năng này, bắt buộc phải thiết lập mật khẩu và thực hiện việc thu hồi chức năng này khi sử dụng xong.

7. Không tự ý cắm thiết bị USB khi máy tính đã nhiễm virus.

8. Bộ phận công nghệ thông tin có toàn quyền truy cập từ xa đến tất cả máy

tính trong Trung tâm Y tế nếu xét thấy cần thiết trong công tác bảo vệ an toàn mạng nội bộ.

9. Viên chức người lao động trong Trung tâm Y tế phối hợp chặt chẽ với Bộ phận công nghệ thông tin, không cản trở gây khó khăn khi Bộ phận công nghệ thông tin thực hiện nhiệm vụ.

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

1.Bảo đảm cho mạng kết nối đến máy chủ, hệ điều hành trên máy chủ, phần mềm cài đặt trên máy chủ hoạt động liên tục, ổn định và an toàn.

2. Không cài đặt các phần mềm không liên quan đến hệ thống thông tin trên máy chủ cài đặt hệ thống thông tin.

3. Máy chủ phải thường xuyên được thiết lập tự động cập nhật các bản vá lỗi hệ điều hành của nhà sản xuất. Nhật ký máy chủ phải lưu trữ ít nhất 01 tháng.

4. Phải thay đổi tài khoản, mật khẩu mặc định khi đưa hệ điều hành trên máy chủ vào sử dụng. Loại bỏ các tài khoản không còn sử dụng khỏi máy chủ.

5. Mỗi tài khoản truy cập các hệ thống thông tin chỉ được cấp cho một người quản lý và sử dụng. Người sử dụng phải có trách nhiệm bảo vệ tài khoản truy cập của mình.

6. Phòng máy chủ là khu vực hạn chế tiếp cận chỉ những cá nhân có quyền, nhiệm vụ theo quy định mới được phép vào phòng máy chủ. Việc vào, ra phòng máy chủ phải được kiểm soát bằng thiết bị bảo vệ (quẹt thẻ, vân tay, sinh trắc học)

Điều 11. Quản lý an toàn dữ liệu

1. Các khoa, phòng, trung tâm được giao chủ trì quản lý, sử dụng hệ thống thông tin nào có trách nhiệm tự sao lưu dữ liệu cá nhân phục vụ công tác chuyên môn.

2. Với các dữ liệu của hệ thống thông tin nghiệp vụ dùng chung trong toàn Trung tâm Y tế, Phòng Kế hoạch Nghiệp vụ có trách nhiệm sao lưu dự phòng vào thiết bị lưu trữ chuyên dụng.

3. Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ và các dữ liệu quan trọng khác trên hệ thống (nếu có).

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

1. Không cài đặt các phần mềm không rõ nguồn gốc, không liên quan đến công việc chuyên môn trên máy tính của cơ quan.

2. Máy trạm phải được đặt mật khẩu truy cập và thiết lập chế độ tự động bảo vệ màn hình sau 15 phút không sử dụng. Trường hợp không sử dụng trong thời gian quá 02 giờ trở lên phải tắt máy để bảo đảm an toàn.

3. Mỗi công chức, viên chức và người lao động phải tự đặt mật khẩu đăng nhập vào các hệ thống thông tin có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số và ký tự đặc biệt như !, @, #, $, %, ...) và

thường xuyên thay đổi để tăng cường công tác bảo mật.(đối với những máy cá nhân)

4. Công chức, viên chức và người lao động có trách nhiệm triển khai các biện pháp phòng chống mã độc theo hướng dẫn của Bộ phận công nghệ thông tin, các đơn vị chuyên trách về an toàn an ninh thông tin.

5. Không tự ý gỡ bỏ các phần mềm phòng chống mã độc trên máy tính. Các phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật. Tất cả các tập tin, thư mục khi sao chép vào máy tính từ thiết bị ngoại vi phải được quét mã độc trước khi thực hiện.

6. Không truy cập vào các hệ thống thông tin công cộng không rõ về nội dung hoặc có nội dung phản cảm, không phù hợp với thuần phong mỹ tục của Việt Nam. Không đọc thư điện tử hoặc tải tệp tin đính kèm trong thư không rõ người gửi; Không kích hoạt các đường liên kết có dấu hiệu không rõ ràng.

Điều 13. Quản lý sự cố

1. Phân loại mức độ nghiêm trọng của các sự cố, bao gồm:

a) Thấp: Sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của các khoa, phòng thuộc Trung tâm Y tế Hà Tiên.

b) Trung bình: Sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hay đình trệ hoạt động chính của các khoa, phòng thuộc Trung tâm Y tế Hà Tiên .

c) Cao: Sự cố làm cho thiết bị, phần mềm hay hệ thống không thể sử dụng được và gây ảnh hưởng đến một trong các hoạt động chính của các khoa, phòng thuộc Trung tâm Y tế Hà Tiên.

d) Nghiêm trọng: Sự cố ảnh hưởng liên tục đến nhiều hoạt động chính của các khoa, phòng thuộc Trung tâm Y tế Hà Tiên.

2. Xử lý sự cố:

a) Khi có sự cố tại Điểm a, b, Khoản 1 Điều này, công chức, viên chức, người lao động có trách nhiệm báo với Bộ phận công nghệ thông tin để để kịp thời xử lý.

b) Khi có sự cố tại Điểm c, Khoản 1 Điều này, công chức, viên chức, người lao động có trách nhiệm báo với Bộ phận công nghệ thông tin và Ban giám đốc Trung tâm Y tế để xin ý kiến chỉ đạo xử lý kịp thời.

c) Đối với sự cố quy định tại Điểm d, Khoản 1 Điều này, Phòng Kế hoạch Nghiệp vụ báo cáo Giám đốc Trung tâm Y tế để xin ý kiến chỉ đạo xử lý kịp thời.

d) Bộ phận công nghệ thông tin có trách nhiệm tham mưu chính sách, quy trình quản lý sự cố an toàn thông tin.

Điều 14. Kiểm tra, đánh giá và quản lý rủi ro

1. Nội dung kiểm tra, đánh giá và quản lý rủi ro an toàn thông tin

a) Kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ.

b) Đánh giá hiệu quả của biện pháp bảo đảm an toàn hệ thống thông tin.

c) Đánh giá phát hiện mã độc, lỗ hổng hệ thống.

d) Kiểm tra, đánh giá khác do chủ quản hệ thống thông tin quv định.

2. Hình thức kiểm tra, đánh giá và quản lý rủi ro an toàn thông tin

a) Định kỳ theo kế hoạch của chủ quản hệ thống thông tin.

b) Kiểm tra, đánh giá đột xuất theo yêu cầu của cấp có thẩm quvền.

Điều 15. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

Hệ thống thông tin khi kết thúc vận hành, khai thác hoặc thanh lý, hủy bỏ phải tuân thủ các quy định của Pháp luật về quản lý tài sản. Thông tin, dữ liệu trên các hệ thống thông tin phải được sao lưu và chuyển sang các hệ thống khác (nếu còn giá trị sử dụng). Thực hiện các biện pháp xóa, hủy dữ liệu trước khi thanh lý, hủy bỏ tài sản.

CHƯƠNG IV
TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 16. Trách nhiệm của Phòng Kế hoạch Nghiệp vụ

1. Chủ trì tham mưu các nhiệm vụ về bảo đảm an toàn thông tin mạng trong triển khai ứng dụng công nghệ thông tin phục vụ hoạt động của Trung tâm Y tế Hà Tiên.

2. Chủ trì tham mưu thẩm định hồ sơ cấp độ an toàn hệ thống thông tin của các hệ thống thông tin do Trung tâm Y tế vận hành hệ thống đề xuất triển khai.

3. Hướng dẫn, hỗ trợ, khuyến cáo các rủi ro do mã độc gây ra cho công chức, viên chức, người lao động trong toàn Trrung tâm Y tế.

4. Thường xuyên cập nhật các quy định mới về bảo đảm an toàn thông tin mạng trong quá trình vận hành hệ thống; đề xuất phương án bảo đảm an toàn thông tin cho hệ thống mạng và các hệ thống thông tin khi có thay đổi về thiết kế.

5. Định kỳ 03 năm hoặc khi có thay đổi chính sách an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung.

6. Cung cấp thông tin, dữ liệu phục vụ thanh tra, kiểm tra, giải quyết khiếu nại, tố cáo về bảo đảm an toàn thông tin khi cấp có thẩm quyền yêu cầu.

7. Tham mưu, đề xuất với Lãnh đạo Trung tâm Y tế biện pháp quản lý, vận hành; nâng cấp hệ thống mạng nội bộ và triển khai các biện pháp bảo đảm an toàn thông tin đáp ứng nhiệm vụ chuyển đổi số phục vụ hoạt động khám, chữa bệnh, quản lý, điều hành của Trung tâm Y tế.

Điều 17. Trách nhiệm của Phòng Tổ chức Hành chánh

1. Sau khi tuyển dụng, tiếp nhận nhân sự mới, Phòng có trách nhiệm phổ biến cho nhân sự mới các quy định về bảo đảm an toàn, an ninh thông tin của

Trung tâm Y tế.

2. Đối với các vị trí tiếp xúc, quản lý các thông tin, dữ liệu quan trọng hoặc quản trị các hệ thống thông tin quan trọng, phải yêu cầu nhân sự mới cam kết bảo mật thông tin bằng văn bản hoặc cam kết trong hợp đồng làm việc, hợp đồng lao động.

3. Giám sát, nhắc nhở công chức, viên chức, người lao động thay đổi mật khẩu thường xuyên.

4. Chủ trì phối hợp với Phòng Kế hoạch Nghiệp vụ khi viên chức và người lao động chấm dứt hoặc thay đổi công việc. Phải thu hồi các tài khoản, quyền truy cập hệ thống, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sử hữu của Trung tâm Y tế Hà Tiên.

Điều 18. Trách nhiệm của các khoa, phòng trực thuộc Trung tâm Y tế

1. Trưởng các khoa, phòng có trách nhiệm tổ chức thực hiện Quy định này và chịu trách nhiệm trong công tác bảo đảm an toàn thông tin của khoa, phòng.

2. Thường xuyên quán triệt các quy định về an toàn thông tin mạng để nâng cao nhận thức về trách nhiệm bảo đảm an toàn thông tin.

3. Phân công cán bộ làm đầu mối phối hợp với Bộ phận công nghệ thông tin theo dõi, xử lý các sự cố an toàn thông tin của khoa, phòng trong Trung tâm Y tế.

4. Phối hợp, cung cấp thông tin và tạo điều kiện để Bộ phận công nghệ thông tin hoặc các đơn vị có thẩm quyền triển khai công tác kiểm tra, khắc phục sự cố an toàn thông tin kịp thời, nhanh chóng và đạt hiệu quả.

Điều 19. Trách nhiệm của công chức và người lao động trong Trung tâm Y tế

1. Nghiêm túc chấp hành quy định này và các quy định khác của pháp luật về an toàn thông tin. Chịu trách nhiệm bảo đảm an toàn thông tin trong phạm vi trách nhiệm và quyền hạn được giao.

2. Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin phải báo cáo ngay với cấp trên và Bộ phận công nghệ thông tin để kịp thời ngăn chặn và xử lý.

3. Tham gia đầy đủ các chương trình diễn tập, tập huấn về an toàn thông tin mạng do các cơ quan chuyên trách về an toàn, an ninh thông tin tổ chức./.

GIÁM ĐỐC

PHÓ GIÁM ĐỐC

SỞ Y TẾ TỈNH AN GIANG
TRUNG TÂM Y TẾ HÀ TIÊN

Nguyễn Hiếu Nghĩa