SỞ Y TẾ TP HỒ CHÍ MINH
TRUNG TÂM Y TẾ
KHU VỰC THUẬN AN

Số: 1327/KH-TTYT

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

Lái Thiêu, ngày 16 tháng 10 năm 2026

KẾ HOẠCH
Bảo đảm an toàn thông tin mạng tại Trung tâm Y tế khu vực Thuận An năm 2026

Căn cứ Chỉ thị số 57-CT/TW ngày 31 tháng 12 năm 2025 của Ban Bí thư về tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị;

Căn cứ Kế hoạch số 191/KH-TBANM ngày 15 tháng 5 năm 2026 của Tiểu ban An toàn thông tin mạng Thành phố về bảo đảm an toàn thông tin mạng trong toàn hệ thống chính trị Thành phố Hồ Chí Minh năm 2026;

Căn cứ Kế hoạch số 14775/KH-SYT của Sở Y tế Thành phố Hồ Chí Minh về bảo đảm an toàn thông tin mạng ngành Y tế Thành phố Hồ Chí Minh năm 2026;

Căn cứ Kế hoạch số 196/ KH-TTYT của Trung tâm Y tế khu vực Thuận An ngày 25/2/2026 về Hoạt động Công nghệ tin trong khám bệnh, chữa bệnh 2026 tại Trung tâm Y tế khu vực Thuận An;

Căn cứ chức năng, nhiệm vụ, quyền hạn và tình hình thực tế về ứng dụng công nghệ thông tin, chuyển đổi số tại Trung tâm Y tế khu vực Thuận An;

Trung tâm Y tế khu vực Thuận An thực hiện xây dựng Kế hoạch bảo đảm an toàn thông tin mạng năm 2026 với các nội dung cụ thể như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Tăng cường công tác bảo đảm an toàn thông tin mạng đối với các hệ thống thông tin, hạ tầng công nghệ thông tin và các phần mềm phục vụ công tác quản lý, điều hành, khám bệnh, chữa bệnh và các hoạt động chuyên môn của Trung tâm.

- Bảo đảm an toàn, bảo mật và tính toàn vẹn, sẵn sàng của dữ liệu; đặc biệt chú trọng bảo vệ dữ liệu cá nhân, dữ liệu sức khỏe, hồ sơ bệnh án và các thông tin liên quan đến người bệnh.

- Chủ động phòng ngừa, phát hiện, ngăn chặn và xử lý kịp thời các nguy cơ mất an toàn thông tin mạng, phần mềm độc hại, mã độc tống tiền, thư điện tử giả mạo, truy cập trái phép và các hình thức tấn công mạng khác.

- Nâng cao nhận thức, trách nhiệm và kỹ năng của viên chức, người lao động trong việc sử dụng hệ thống thông tin, khai thác dữ liệu và thực hiện các quy định về bảo đảm an toàn thông tin mạng.

- Tăng cường khả năng ứng phó sự cố, duy trì hoạt động liên tục của các hệ thống thông tin thiết yếu, hạn chế tối đa ảnh hưởng đến hoạt động chuyên môn và công tác phục vụ người bệnh.

2. Yêu cầu

- Triển khai thực hiện nghiêm túc, đồng bộ, có trọng tâm, trọng điểm và phù hợp với kế hoạch của Sở Y tế Thành phố Hồ Chí Minh về bảo đảm an toàn thông tin mạng năm 2026.

- Xác định rõ trách nhiệm của các khoa, phòng, bộ phận và cá nhân trong quản lý, vận hành, khai thác hệ thống thông tin và bảo vệ dữ liệu thuộc phạm vi được giao.

- Thực hiện các biện pháp bảo đảm an toàn thông tin mạng theo cấp độ của hệ thống thông tin đã được phê duyệt; thường xuyên rà soát, đánh giá nguy cơ và khắc phục các điểm yếu, lỗ hổng bảo mật.

- Kết hợp các giải pháp kỹ thuật, quản lý, đào tạo, tuyên truyền và kiểm tra; ưu tiên bảo vệ các hệ thống phục vụ khám bệnh, chữa bệnh và các hệ thống có chứa dữ liệu sức khỏe cá nhân.

- Việc triển khai các biện pháp bảo đảm an toàn thông tin mạng không làm gián đoạn hoạt động khám bệnh, chữa bệnh; bảo đảm khả năng khôi phục hệ thống khi xảy ra sự cố.

- Các nhiệm vụ phải được thực hiện theo chức năng, nhiệm vụ, thẩm quyền, nguồn lực và điều kiện thực tế của Trung tâm; bảo đảm tiết kiệm, hiệu quả và tuân thủ quy định pháp luật.

II. MỤC TIÊU

1. Mục tiêu chung

- Bảo đảm an toàn thông tin mạng đối với các hệ thống thông tin phục vụ công tác quản lý, chỉ đạo, điều hành và chuyên môn nghiệp vụ tại Trung tâm.

- Bảo vệ dữ liệu y tế, dữ liệu cá nhân và các thông tin quan trọng; phòng ngừa nguy cơ rò rỉ, mất mát, thay đổi hoặc truy cập, sử dụng dữ liệu trái phép.

- Tăng cường năng lực phòng, chống mã độc; chủ động phát hiện, ngăn chặn và xử lý các nguy cơ, sự cố an toàn thông tin mạng.

- Từng bước hoàn thiện quy trình quản lý, vận hành, giám sát, sao lưu, khôi phục dữ liệu và ứng phó sự cố an toàn thông tin mạng tại đơn vị.

2. Mục tiêu cụ thể

- 100% hệ thống thông tin thuộc phạm vi quản lý của Trung tâm được rà soát, thống kê và đánh giá hiện trạng an toàn thông tin mạng; xác định các hệ thống cần phân loại, xác định hoặc rà soát cấp độ an toàn thông tin theo quy định.

- 100% máy trạm thuộc phạm vi quản lý được rà soát và triển khai giải pháp phòng, chống mã độc phù hợp với điều kiện kỹ thuật và yêu cầu của cơ quan quản lý.

- Các tài khoản truy cập hệ thống thông tin được quản lý theo nhiệm vụ, quyền hạn; thực hiện rà soát, điều chỉnh hoặc thu hồi quyền truy cập khi có thay đổi vị trí công tác, nghỉ việc hoặc không còn nhu cầu sử dụng.

- Các hệ thống thông tin quan trọng được thực hiện sao lưu dữ liệu định kỳ, có phương án khôi phục dữ liệu và kiểm tra khả năng phục hồi theo kế hoạch của đơn vị.

- 100% khoa, phòng và bộ phận có liên quan được phổ biến các quy định cơ bản về bảo đảm an toàn thông tin mạng, bảo vệ dữ liệu cá nhân và trách nhiệm báo cáo khi phát hiện dấu hiệu bất thường.

- Các sự cố an toàn thông tin mạng được tiếp nhận, ghi nhận, báo cáo và xử lý kịp thời theo quy trình; không tự ý xóa dấu vết, che giấu hoặc làm sai lệch thông tin về sự cố.

- Cử viên chức phụ trách công nghệ thông tin hoặc an toàn thông tin mạng tham gia các lớp tập huấn, đào tạo, diễn tập do Sở Y tế và cơ quan có thẩm quyền tổ chức.

- Các chỉ tiêu nêu trên là mục tiêu phấn đấu của Trung tâm; việc đánh giá kết quả căn cứ vào phạm vi hệ thống thực tế, hiện trạng triển khai và yêu cầu của Sở Y tế.

III. NHIỆM VỤ VÀ GIẢI PHÁP THỰC HIỆN

1. Tăng cường công tác quản lý, chỉ đạo và tổ chức thực hiện

- Tổ chức quán triệt, phổ biến nội dung kế hoạch của Sở Y tế và Kế hoạch này đến các khoa, phòng, bộ phận, viên chức và người lao động trong toàn Trung tâm.

- Phân công lãnh đạo phụ trách công tác bảo đảm an toàn thông tin mạng; xác định đầu mối phụ trách công nghệ thông tin, tiếp nhận thông tin và phối hợp xử lý sự cố.

- Rà soát, ban hành hoặc cập nhật các quy định nội bộ về quản lý, sử dụng máy tính, mạng nội bộ, thư điện tử công vụ, tài khoản truy cập, phần mềm chuyên môn và các thiết bị lưu trữ dữ liệu.

- Lồng ghép yêu cầu bảo đảm an toàn thông tin mạng vào hoạt động quản lý, vận hành, bảo trì, nâng cấp và triển khai các hệ thống công nghệ thông tin của Trung tâm.

2. Rà soát, thống kê và phân loại cấp độ hệ thống thông tin

- Thống kê các hệ thống thông tin, phần mềm, máy trạm, thiết bị mạng, đường truyền Internet và thiết bị lưu trữ dữ liệu thuộc phạm vi quản lý của Trung tâm.

- Rà soát các hệ thống phục vụ khám bệnh, chữa bệnh, quản lý hồ sơ bệnh án, quản lý dược, xét nghiệm, chẩn đoán hình ảnh, quản lý viện phí, bảo hiểm y tế, quản lý nhân sự và các hệ thống nghiệp vụ khác đang được triển khai tại đơn vị.

- Xác định phạm vi dữ liệu được thu thập, lưu trữ, xử lý và chia sẻ; đánh giá mức độ quan trọng của từng hệ thống, nguy cơ ảnh hưởng đến hoạt động chuyên môn khi hệ thống bị gián đoạn.

- Thực hiện phân loại, xác định cấp độ an toàn hệ thống thông tin, lập hồ sơ đề xuất cấp độ hoặc rà soát, cập nhật hồ sơ theo quy định và hướng dẫn của cơ quan có thẩm quyền.

- Xây dựng phương án bảo đảm an toàn thông tin theo cấp độ được phê duyệt; phối hợp với đơn vị cung cấp phần mềm và các cơ quan liên quan khắc phục các tồn tại, hạn chế được phát hiện.

3. Bảo vệ hạ tầng công nghệ thông tin và máy trạm

- Rà soát tình trạng hoạt động, cấu hình bảo mật và việc cập nhật hệ điều hành, phần mềm trên máy trạm và thiết bị mạng.

- Triển khai, duy trì giải pháp phòng, chống mã độc phù hợp; bảo đảm các thiết bị thuộc phạm vi quản lý được cập nhật cơ sở dữ liệu nhận diện mã độc theo khả năng kỹ thuật và điều kiện triển khai.

- Kiểm soát việc cài đặt phần mềm, sử dụng thiết bị lưu trữ ngoài và kết nối các thiết bị không thuộc danh mục được phép sử dụng.

- Thực hiện thay đổi mật khẩu mặc định, sử dụng mật khẩu có độ an toàn phù hợp, bật xác thực nhiều yếu tố đối với các hệ thống hỗ trợ và có mức độ rủi ro cao.

- Rà soát quyền truy cập của tài khoản quản trị, tài khoản người dùng và tài khoản của đơn vị cung cấp dịch vụ; hạn chế sử dụng chung tài khoản và không chia sẻ thông tin xác thực.

- Cấu hình tường lửa, phân tách mạng và kiểm soát kết nối phù hợp với điều kiện thực tế; hạn chế truy cập từ bên ngoài đối với các hệ thống nội bộ nếu không có nhu cầu nghiệp vụ được phê duyệt.

- Tắt hoặc gỡ bỏ các dịch vụ, cổng kết nối và phần mềm không cần thiết; thực hiện cập nhật bản vá bảo mật theo mức độ rủi ro và hướng dẫn của nhà sản xuất, đơn vị quản lý hệ thống.

- Tăng cường kiểm soát truy cập vật lý đối với phòng máy chủ, thiết bị mạng và khu vực lưu trữ dữ liệu quan trọng.

4. Bảo vệ dữ liệu y tế và dữ liệu cá nhân

- Thực hiện quản lý, khai thác, sử dụng, lưu trữ và chia sẻ dữ liệu theo đúng mục đích, thẩm quyền và quy định pháp luật.

- Xác định rõ trách nhiệm của các khoa, phòng, cá nhân được giao quản lý hoặc sử dụng dữ liệu; chỉ cấp quyền truy cập phù hợp với nhiệm vụ được phân công.

- Không tự ý sao chép, cung cấp, gửi hoặc công khai hồ sơ bệnh án, thông tin sức khỏe, dữ liệu cá nhân của người bệnh và dữ liệu nội bộ cho tổ chức, cá nhân không có thẩm quyền.

- Sử dụng các kênh truyền nhận dữ liệu được đơn vị cho phép; hạn chế lưu trữ dữ liệu chuyên môn trên thiết bị cá nhân, tài khoản thư điện tử cá nhân hoặc các nền tảng lưu trữ trực tuyến chưa được phê duyệt.

- Rà soát việc chia sẻ dữ liệu với đơn vị cung cấp phần mềm, đơn vị hỗ trợ kỹ thuật và các hệ thống liên thông; bảo đảm có cơ sở, phạm vi và biện pháp bảo vệ phù hợp.

- Thực hiện các biện pháp bảo vệ dữ liệu trong quá trình thu thập, xử lý, lưu trữ, truyền đưa và tiêu hủy; lưu giữ nhật ký truy cập đối với các hệ thống có chức năng hỗ trợ.

- Khi phát hiện nguy cơ lộ, mất hoặc sử dụng dữ liệu trái phép, cá nhân phát hiện phải báo ngay cho lãnh đạo phụ trách và đầu mối công nghệ thông tin để xử lý, báo cáo theo quy định.

5. Sao lưu dữ liệu và bảo đảm hoạt động liên tục

- Xây dựng danh mục dữ liệu cần sao lưu, xác định tần suất sao lưu và thời gian lưu giữ phù hợp với mức độ quan trọng của từng hệ thống.

- Ưu tiên sao lưu dữ liệu của các hệ thống phục vụ khám bệnh, chữa bệnh, hồ sơ bệnh án, xét nghiệm, chẩn đoán hình ảnh và các dữ liệu nghiệp vụ quan trọng khác.

- Bảo đảm bản sao lưu được quản lý an toàn, hạn chế quyền truy cập; nghiên cứu áp dụng bản sao lưu tách biệt với hệ thống đang vận hành để giảm nguy cơ bị mã hóa hoặc xóa đồng thời khi xảy ra tấn công mạng.

- Kiểm tra định kỳ tình trạng bản sao lưu và thực hiện thử nghiệm khôi phục dữ liệu theo kế hoạch, bảo đảm dữ liệu có thể sử dụng khi cần thiết.

- Xây dựng phương án duy trì hoạt động chuyên môn khi hệ thống công nghệ thông tin bị gián đoạn, bao gồm phương án tiếp nhận người bệnh, ghi nhận thông tin và cập nhật dữ liệu sau khi hệ thống được khôi phục.

- Phối hợp với đơn vị cung cấp phần mềm, đơn vị vận hành hạ tầng và cơ quan quản lý để khắc phục sự cố, khôi phục hệ thống và bảo đảm tính liên tục của hoạt động khám bệnh, chữa bệnh.

6. Giám sát, kiểm tra và đánh giá an toàn thông tin mạng

- Thường xuyên theo dõi tình trạng hoạt động của hệ thống thông tin, máy trạm, thiết bị mạng và phần mềm phòng, chống mã độc.

- Rà soát nhật ký hệ thống, cảnh báo bảo mật, dấu hiệu truy cập bất thường, tài khoản đăng nhập không hợp lệ và các biểu hiện nghi ngờ bị tấn công mạng.

- Tổ chức kiểm tra nội bộ việc thực hiện các quy định về quản lý tài khoản, sử dụng thiết bị, sao lưu dữ liệu, cập nhật phần mềm và bảo vệ dữ liệu cá nhân.

- Phối hợp với Sở Y tế và các đơn vị chuyên trách để thực hiện kiểm tra, đánh giá, quét lỗ hổng bảo mật hoặc rà soát mã độc khi có yêu cầu và trong phạm vi được phép.

- Kịp thời lập danh sách các tồn tại, xác định mức độ ảnh hưởng, phân công bộ phận khắc phục và theo dõi kết quả xử lý.

- Không tự ý thực hiện quét, kiểm thử xâm nhập hoặc các hoạt động kỹ thuật có khả năng ảnh hưởng đến hệ thống đang phục vụ khám bệnh, chữa bệnh khi chưa được phê duyệt.

7. Xây dựng và triển khai phương án ứng phó sự cố

- Rà soát, xây dựng hoặc cập nhật quy trình ứng phó sự cố an toàn thông tin mạng phù hợp với quy trình của cơ quan quản lý cấp trên.

- Xác định đầu mối tiếp nhận thông tin, người chịu trách nhiệm chỉ đạo, bộ phận kỹ thuật phối hợp và các đơn vị liên quan trong quá trình xử lý sự cố.

- Khi phát hiện sự cố, thực hiện các bước tiếp nhận thông tin, đánh giá sơ bộ, cô lập phạm vi bị ảnh hưởng khi cần thiết, bảo toàn dữ liệu và nhật ký liên quan, khắc phục nguyên nhân và khôi phục hoạt động.

- Đối với sự cố có nguy cơ ảnh hưởng đến dữ liệu sức khỏe, hồ sơ bệnh án, nhiều hệ thống hoặc hoạt động khám bệnh, chữa bệnh, phải báo cáo ngay lãnh đạo Trung tâm và thông báo cơ quan có thẩm quyền theo quy định.

- Không tự ý xóa dữ liệu, cài đặt lại thiết bị, định dạng ổ đĩa hoặc thực hiện thao tác làm mất dấu vết sự cố trước khi có phương án xử lý phù hợp.

- Phối hợp với Sở Y tế, cơ quan chuyên trách về an toàn thông tin mạng, an ninh mạng và đơn vị cung cấp dịch vụ để xử lý sự cố khi vượt quá khả năng của Trung tâm.

- Sau sự cố, tổ chức đánh giá nguyên nhân, phạm vi ảnh hưởng, thiệt hại và biện pháp khắc phục; đề xuất giải pháp phòng ngừa tái diễn.

8. Đào tạo, tập huấn và tuyên truyền nâng cao nhận thức

- Tổ chức phổ biến các quy định pháp luật, quy chế nội bộ và hướng dẫn về bảo đảm an toàn thông tin mạng đến viên chức, người lao động.

- Hướng dẫn kỹ năng nhận diện thư điện tử giả mạo, liên kết độc hại, tệp đính kèm nguy hiểm, hành vi lừa đảo trực tuyến và các hình thức đánh cắp tài khoản.

- Tuyên truyền việc sử dụng mật khẩu an toàn, bảo vệ thiết bị, khóa máy tính khi rời vị trí làm việc, không chia sẻ tài khoản và không sử dụng phần mềm không rõ nguồn gốc.

- Hướng dẫn nhân viên y tế và nhân viên hành chính thực hiện đúng quy định về bảo mật thông tin người bệnh, hồ sơ bệnh án và dữ liệu cá nhân.

- Cử nhân sự phụ trách công nghệ thông tin và các viên chức có liên quan tham gia đầy đủ các lớp tập huấn, đào tạo, diễn tập do Sở Y tế và cơ quan có thẩm quyền tổ chức.

- Lồng ghép nội dung an toàn thông tin mạng vào các cuộc họp giao ban, sinh hoạt chuyên môn và hoạt động đào tạo nội bộ của Trung tâm.

9. Hoàn thiện quy chế nội bộ và quản lý nhà cung cấp dịch vụ

- Rà soát các quy định nội bộ liên quan đến quản lý, sử dụng hệ thống thông tin, thiết bị công nghệ thông tin, tài khoản người dùng và dữ liệu.

- Quy định rõ trách nhiệm của cá nhân được cấp tài khoản, trách nhiệm quản lý thiết bị, việc sử dụng thiết bị lưu trữ ngoài và nghĩa vụ báo cáo sự cố.

- Đối với các hệ thống do đơn vị bên ngoài cung cấp hoặc vận hành, rà soát trách nhiệm bảo đảm an toàn thông tin, sao lưu, khôi phục, quản lý tài khoản hỗ trợ kỹ thuật và xử lý sự cố theo hợp đồng, thỏa thuận và quy định pháp luật.

- Kiểm soát việc cấp quyền truy cập từ xa cho đơn vị hỗ trợ kỹ thuật; chỉ thực hiện khi có nhu cầu, được phê duyệt, có biện pháp kiểm soát và thu hồi quyền sau khi hoàn thành công việc.

- Rà soát các yêu cầu bảo mật khi mua sắm, thuê dịch vụ, nâng cấp hoặc thay thế thiết bị, phần mềm và hệ thống thông tin.

10. Bảo đảm kinh phí và nguồn lực thực hiện

- Căn cứ nhiệm vụ được giao, hiện trạng hệ thống và yêu cầu thực tế, các khoa, phòng đề xuất nhu cầu kinh phí bảo đảm an toàn thông tin mạng gửi bộ phận được giao tổng hợp.

- Ưu tiên bố trí nguồn lực cho các nhiệm vụ thiết yếu như phòng, chống mã độc, sao lưu và khôi phục dữ liệu, cập nhật bảo mật, bảo trì hệ thống, đào tạo và ứng phó sự cố.

- Việc lập dự toán, quản lý và sử dụng kinh phí thực hiện theo quy định pháp luật, dự toán được giao và khả năng cân đối nguồn lực của Trung tâm.

- Khuyến khích tận dụng hiệu quả hạ tầng hiện có, phối hợp sử dụng các giải pháp kỹ thuật do cơ quan quản lý cấp trên triển khai, tránh đầu tư trùng lặp và bảo đảm hiệu quả.

IV. TIẾN ĐỘ THỰC HIỆN

1. Giai đoạn triển khai kế hoạch

- Tổ chức phổ biến kế hoạch; phân công nhiệm vụ và xác định đầu mối phụ trách an toàn thông tin mạng.

- Rà soát, thống kê hệ thống thông tin, thiết bị công nghệ thông tin, tài khoản người dùng và hiện trạng bảo vệ dữ liệu.

- Xây dựng danh mục nhiệm vụ cần thực hiện, xác định mức độ ưu tiên, dự kiến kinh phí và nhân lực.

2. Giai đoạn triển khai thường xuyên

- Duy trì cập nhật phần mềm, phòng chống mã độc, quản lý tài khoản, kiểm soát truy cập và sao lưu dữ liệu.

- Tổ chức tuyên truyền, hướng dẫn, tập huấn; kiểm tra việc thực hiện các quy định về an toàn thông tin mạng.

- Thực hiện các nhiệm vụ theo yêu cầu của Sở Y tế và cơ quan có thẩm quyền; báo cáo ngay khi xảy ra sự cố hoặc có yêu cầu đột xuất.

3. Giai đoạn rà soát, tổng kết

- Đánh giá kết quả thực hiện các mục tiêu, nhiệm vụ; tổng hợp các tồn tại, hạn chế và nguyên nhân.

- Rà soát tình trạng khắc phục các nguy cơ, điểm yếu và kiến nghị giải pháp tiếp tục thực hiện.

- Tổng hợp kết quả, lập báo cáo gửi Sở Y tế theo thời hạn và biểu mẫu được hướng dẫn; đề xuất nhiệm vụ bảo đảm an toàn thông tin mạng cho năm tiếp theo.

- Tiến độ cụ thể được thực hiện theo yêu cầu của Sở Y tế và lịch công tác của Trung tâm; các nhiệm vụ thường xuyên phải được duy trì trong suốt năm 2026.

V. PHÂN CÔNG TỔ CHỨC THỰC HIỆN

1. Ban Giám đốc Trung tâm

- Chỉ đạo chung việc triển khai, kiểm tra và đánh giá kết quả thực hiện kế hoạch tại Trung tâm.

- Phân công lãnh đạo phụ trách, chỉ đạo xử lý các vấn đề phát sinh và quyết định biện pháp ứng phó khi xảy ra sự cố thuộc thẩm quyền.

- Chỉ đạo bố trí nhân lực, kinh phí và các điều kiện cần thiết để triển khai nhiệm vụ bảo đảm an toàn thông tin mạng.

- Chỉ đạo thực hiện chế độ báo cáo định kỳ, đột xuất với Sở Y tế và cơ quan có thẩm quyền theo quy định.

2. Phòng Kế hoạch Nghiệp vụ

- Là đầu mối tham mưu Ban Giám đốc tổ chức triển khai, theo dõi và tổng hợp kết quả thực hiện kế hoạch.

- Rà soát, thống kê hệ thống thông tin, máy trạm, thiết bị mạng, phần mềm và các tài khoản truy cập thuộc phạm vi quản lý.

- Tham mưu xây dựng, cập nhật quy trình quản lý, vận hành, sao lưu, khôi phục dữ liệu và ứng phó sự cố an toàn thông tin mạng.

- Theo dõi tình trạng hoạt động của hệ thống, giải pháp phòng chống mã độc, cảnh báo bảo mật; phối hợp xử lý các sự cố kỹ thuật.

- Phối hợp với đơn vị cung cấp phần mềm, đơn vị hỗ trợ kỹ thuật và cơ quan chuyên trách để khắc phục lỗ hổng, xử lý mã độc và phục hồi hệ thống khi cần thiết.

- Thực hiện lưu trữ hồ sơ kỹ thuật, nhật ký kiểm tra, kết quả khắc phục và các tài liệu liên quan; tổng hợp số liệu, tham mưu báo cáo định kỳ và đột xuất.

- Tham mưu đề xuất nhu cầu trang thiết bị, phần mềm, dịch vụ và kinh phí cần thiết để bảo đảm an toàn thông tin mạng.

3. Phòng Tổ chức - Hành chính

- Phối hợp phổ biến các quy định, quy trình và nội dung tuyên truyền về an toàn thông tin mạng đến viên chức, người lao động.

- Phối hợp rà soát thông tin nhân sự phục vụ việc cấp mới, điều chỉnh, thu hồi tài khoản truy cập khi tuyển dụng, điều chuyển, thay đổi nhiệm vụ hoặc chấm dứt công tác.

- Phối hợp quản lý văn bản, hồ sơ, tài liệu liên quan đến công tác bảo đảm an toàn thông tin mạng theo quy định.

4. Phòng Tài chính - Kế toán

- Phối hợp với phòng Kế hoạch Nghiệp vụ và các khoa, phòng tham mưu lập dự toán kinh phí thực hiện các nhiệm vụ bảo đảm an toàn thông tin mạng.

- Tham mưu bố trí, quản lý và sử dụng kinh phí theo dự toán được duyệt, quy định pháp luật và khả năng cân đối nguồn lực của đơn vị.

- Phối hợp thực hiện các thủ tục mua sắm, sửa chữa, bảo trì, thuê dịch vụ công nghệ thông tin theo quy định hiện hành.

5. Các khoa, phòng chuyên môn

- Tổ chức triển khai kế hoạch đến viên chức, người lao động thuộc phạm vi quản lý; chịu trách nhiệm về việc chấp hành quy định bảo đảm an toàn thông tin mạng tại bộ phận.

- Quản lý, sử dụng đúng mục đích các thiết bị, phần mềm và tài khoản được cấp; không tự ý cài đặt phần mềm không rõ nguồn gốc, chia sẻ tài khoản hoặc kết nối thiết bị trái phép vào hệ thống.

- Bảo vệ dữ liệu chuyên môn, dữ liệu người bệnh, hồ sơ bệnh án và các thông tin thuộc phạm vi quản lý; không cung cấp, sao chép hoặc chia sẻ dữ liệu trái thẩm quyền.

- Phối hợp thực hiện việc rà soát tài khoản, thiết bị, dữ liệu và nhu cầu sử dụng hệ thống; kịp thời thông báo khi có thay đổi nhân sự hoặc phát sinh nhu cầu điều chỉnh quyền truy cập.

- Khi phát hiện dấu hiệu bất thường, nghi ngờ nhiễm mã độc, mất thiết bị, lộ thông tin hoặc sự cố hệ thống, phải báo ngay cho lãnh đạo phụ trách và đầu mối công nghệ thông tin để xử lý.

- Cử nhân sự tham gia đầy đủ các chương trình đào tạo, tập huấn, tuyên truyền và diễn tập theo kế hoạch.

6. Viên chức, người lao động

- Chấp hành nghiêm các quy định về an toàn thông tin mạng, bảo vệ dữ liệu cá nhân và bảo mật thông tin người bệnh.

- Không cung cấp mật khẩu, mã xác thực hoặc thông tin truy cập cho người khác; không sử dụng tài khoản của người khác khi chưa được phép.

- Không mở các tệp đính kèm, liên kết đáng ngờ; không cài đặt phần mềm không được phép và không sử dụng thiết bị cá nhân để lưu trữ dữ liệu công việc trái quy định.

- Chủ động tham gia các hoạt động tuyên truyền, tập huấn; báo cáo kịp thời các nguy cơ, hành vi vi phạm và sự cố an toàn thông tin mạng.

7. Đơn vị cung cấp phần mềm, dịch vụ công nghệ thông tin

- Phối hợp với Trung tâm trong việc bảo trì, cập nhật, khắc phục lỗ hổng, sao lưu và khôi phục hệ thống theo phạm vi hợp đồng, thỏa thuận và quy định pháp luật.

- Thực hiện nghiêm các yêu cầu về bảo mật, quản lý tài khoản hỗ trợ kỹ thuật, bảo vệ dữ liệu và xử lý sự cố.

- Thông báo kịp thời cho Trung tâm khi phát hiện nguy cơ ảnh hưởng đến an toàn thông tin hoặc hoạt động của hệ thống thuộc phạm vi cung cấp dịch vụ.

VI. CHẾ ĐỘ THÔNG TIN, BÁO CÁO

1. Báo cáo định kỳ

- Các khoa, phòng và bộ phận liên quan báo cáo tình hình thực hiện nhiệm vụ, các tồn tại và kiến nghị về phòng Kế hoạch Nghiệp vụ theo yêu cầu của Trung tâm.

- Phòng Kế hoạch Nghiệp vụ tổng hợp kết quả thực hiện kế hoạch, tham mưu Ban Giám đốc báo cáo Sở Y tế theo thời hạn, biểu mẫu và nội dung được hướng dẫn.

- Nội dung báo cáo bao gồm: kết quả thực hiện các nhiệm vụ; tình hình rà soát, phân loại cấp độ hệ thống thông tin; tình trạng triển khai giải pháp phòng, chống mã độc; công tác sao lưu dữ liệu; hoạt động kiểm tra, tập huấn; tình hình sự cố; kết quả khắc phục và kiến nghị, đề xuất.

- Thời hạn báo cáo định kỳ thực hiện theo yêu cầu của Sở Y tế. Trường hợp chưa có lịch báo cáo cụ thể, bộ phận phụ trách công nghệ thông tin tham mưu Ban Giám đốc xác định thời điểm tổng hợp phù hợp.

2. Báo cáo đột xuất và báo cáo sự cố

- Khi xảy ra sự cố an toàn thông tin mạng hoặc phát hiện nguy cơ có thể ảnh hưởng đến hệ thống thông tin, dữ liệu người bệnh và hoạt động khám bệnh, chữa bệnh, bộ phận phát hiện phải báo ngay cho lãnh đạo Trung tâm và đầu mối công nghệ thông tin.

- Phòng Kế hoạch Nghiệp vụ tin tham mưu Ban Giám đốc thực hiện báo cáo, thông báo đến Sở Y tế và cơ quan có thẩm quyền theo quy định, bảo đảm đúng thời hạn và quy trình ứng phó sự cố.

- Báo cáo sự cố phải nêu rõ thời gian phát hiện, hệ thống bị ảnh hưởng, biểu hiện sự cố, phạm vi ảnh hưởng sơ bộ, biện pháp đã thực hiện, tình trạng khắc phục và kiến nghị hỗ trợ.

- Không tự ý cung cấp thông tin về sự cố, dữ liệu người bệnh hoặc thông tin kỹ thuật nhạy cảm cho bên không có thẩm quyền.

3. Tổng kết và lưu trữ hồ sơ

- Cuối kỳ thực hiện, phòng Kế hoạch Nghiệp vụ phối hợp với các khoa, phòng tổng hợp kết quả, đánh giá mức độ hoàn thành các mục tiêu và đề xuất giải pháp cải thiện.

- Hồ sơ thực hiện kế hoạch, báo cáo, biên bản kiểm tra, tài liệu tập huấn, nhật ký sự cố và kết quả khắc phục được quản lý, lưu trữ theo quy định.

VII. KINH PHÍ THỰC HIỆN

- Kinh phí thực hiện kế hoạch được bố trí từ nguồn ngân sách, nguồn kinh phí được giao và các nguồn hợp pháp khác theo quy định pháp luật.

- Các khoa, phòng và bộ phận liên quan căn cứ nhiệm vụ được phân công, chủ động đề xuất nhu cầu kinh phí gửi bộ phận được giao tổng hợp, tham mưu Ban Giám đốc xem xét, quyết định theo thẩm quyền.

- Việc quản lý, sử dụng và thanh quyết toán kinh phí phải bảo đảm đúng mục đích, tiết kiệm, hiệu quả, công khai và tuân thủ quy định hiện hành.

VIII. TỔ CHỨC THỰC HIỆN

- Trưởng các khoa, phòng, bộ phận và toàn thể viên chức, người lao động thuộc Trung tâm Y tế khu vực Thuận An có trách nhiệm nghiêm túc triển khai thực hiện kế hoạch này.

- Phòng Kế hoạch Nghiệp vụ chịu trách nhiệm theo dõi, đôn đốc, tổng hợp tình hình thực hiện; kịp thời tham mưu Ban Giám đốc giải quyết khó khăn, vướng mắc và đề xuất điều chỉnh nhiệm vụ phù hợp với yêu cầu thực tế.

- Trong quá trình thực hiện, nếu có khó khăn, vướng mắc hoặc phát sinh sự cố vượt quá khả năng xử lý, các khoa, phòng, bộ phận kịp thời báo cáo Ban Giám đốc để xem xét, chỉ đạo và báo cáo với Sở Y tế, cơ quan có thẩm quyền giải quyết theo quy định.

Trên đây là Kế hoạch bảo đảm an toàn thông tin mạng tại Trung tâm Y tế khu vực Thuận An năm 2026. Đề nghị các khoa, phòng, bộ phận và toàn thể viên chức, người lao động nghiêm túc triển khai thực hiện./.

Nơi nhận:
- Sở Y tế Thành phố Hồ Chí Minh (báo cáo);
- Ban Giám đốc Trung tâm;
- Các khoa, phòng Trung tâm;
- Lưu: VT, P. KHNV.

GIÁM ĐỐC

SỞ Y TẾ THÀNH PHỐ HỒ CHÍ MINH
TRUNG TÂM Y TẾ KHU VỰC THUẬN AN

Phan Quang Toàn