SỞ Y TẾ BÌNH ĐỊNH **TTYT HUYỆN PHÙ MỸ**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 256 /QĐ-TTYT	*Phù Mỹ, ngày 03 tháng 5 năm 2024*

QUYẾT ĐỊNH
Về việc ban hành Quy chế An toàn thông tin

GIÁM ĐỐC TRUNG TÂM Y TẾ

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

Căn cứ Luật An ninh mạng ngày 17/6/2018;

Căn cứ 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;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định số 2694/QĐ-UBND ngày 22/8/2022 của Ủy ban nhân dân tỉnh Bình Định quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Trung tâm Y tế huyện Phù Mỹ;

Theo đề nghị của Trưởng phòng Kế hoạch - Nghiệp vụ - Điều dưỡng.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế An toàn thông tin trong Trung tâm Y tế huyện Phù Mỹ.

Điều 2. Quy chế An toàn thông tin trong Trung tâm Y tế huyện Phù Mỹ có hiệu lực kể từ ngày ký.

Điều 3. Trưởng phòng Kế hoạch - Nghiệp vụ - Điều dưỡng, Tổ chức - Hành chính, Tài chính - Kế toán và Trưởng khoa, phòng, trạm y tế, tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

***Nơi nhận*:**
- Như Điều 3;
- Sở Y tế (Báo cáo);
- Lãnh đạo TTYT;
- Khoa, phòng, trạm y tế;
- Webside:ttytphumy.com;
- Lưu: VT, KHNV-ĐD

GIÁM ĐỐC

SỞ Y TẾ TỈNH BÌNH ĐỊNH
TRUNG TÂM Y TẾ HUYỆN PHÙ MỸ

Nguyễn Thái Học

QUY CHẾ
BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG TRONG HOẠT ĐỘNG ỨNG DỤNG CÔNG NGHỆ THÔNG TIN TẠI TRUNG TÂM Y TẾ HUYỆN PHÙ MỸ

(Kèm theo Quyết định số /2024/QĐ-TTYT ngày 3 tháng 5 năm 2024 của Trung tâm Y tế Huyện Phù Mỹ)

Chương I

QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định việc bảo đảm an toàn thông tin (ATTT) mạng trong hoạt động ứng dụng công nghệ thông tin trong toàn Trung tâm Y tế (TTYT) huyện Phù Mỹ.

Điều 2. Đối tượng áp dụng

1. Trung tâm tế huyện Phù Mỹ, 19 trạm Y tế xã, thị trấn, cùng toàn thể khoa, phòng tại đơn vị.

2. Viên chức, người lao động (gọi tắt là viên chức) và các tổ chức, cá nhân có liên quan tham gia vận hành, khai thác các hệ thống thông tin tại cơ quan, đơn vị quy định tại khoản 1 Điều này.

3. Các doanh nghiệp cung cấp dịch vụ viễn thông, công nghệ thông tin (CNTT), Internet; các doanh nghiệp, tổ chức, cá nhân có tham gia vào các hoạt động ứng dụng CNTT của các cơ quan, đơn vị thuộc khoản 1 Điều này.

4. Khuyến khích các cơ quan, đơn vị khác hoạt động ứng dụng và phát triển CNTT trên địa bàn huyện áp dụng quy chế này.

Điều 3. Giải thích từ ngữ

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

1. *Nguy cơ mất ATTT mạng* là những nhân tố bên trong hoặc bên ngoài có khả năng ảnh hưởng tới trạng thái ATTT mạng.

2. *Bản ghi nhật ký hệ thống (Logfile)* là một tập tin được tạo ra trên mỗi thiết bị của hệ thống thông tin như: Tường lửa, máy chủ ứng dụng,... có chứa tất cả thông tin về các hoạt động xảy ra trên thiết bị đó. Bản ghi nhật ký hệ thống dùng để phân tích những sự kiện đã xảy ra, nguồn gốc và các kết quả để có các biện pháp xử lý thích hợp.

3. Trung tâm tích hợp dữ liệu tỉnh bao gồm:

a) Phần cứng: thiết bị máy chủ, thiết bị ngoại vi, thiết bị mạng, thiết bị phụ trợ, thiết bị lưu trữ, thiết bị bảo mật, hệ thống Hội nghị truyền hình và các thiết bị khác có liên quan;

b) Hệ thống phần mềm: Hệ thống các ứng dụng được cài đặt, lưu trữ tại Phòng tích hợp dữ liệu của tỉnh;

c) Mạng truyền thông bao gồm: mạng nội bộ, mạng internet (hữu tuyến và vô tuyến), mạng truyền số liệu chuyên dùng, mạng LAN-WAN nội tỉnh;

d) Tài nguyên địa chỉ IP *(Internet Protocol - giao thức Internet)* 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;

đ) Các phân vùng mạng VLAN *(virtual local area network)* là một kỹ thuật cho phép tạo lập các mạng LAN độc lập một cách logic trên cùng một kiến trúc hạ tầng vật lý. Việc tạo lập nhiều mạng LAN ảo trong cùng một mạng cục bộ giúp giảm thiểu miền quảng bá *(broadcast domain)* cũng như tạo thuận lợi cho việc quản lý một mạng cục bộ rộng lớn. VLAN tương đương như mạng con.

Điều 4. Tài nguyên thông tin cần bảo đảm ATTT

Tài nguyên thông tin cần bảo đảm ATTT tại Trung tâm Y tế huyện bao gồm các thành phần sau đây:

1. Hệ thống hạ tầng kỹ thuật:

a) Thiết bị tính toán, lưu trữ (máy chủ, máy trạm, SAN, NAS, DAS, VAS);

b) Thiết bị ngoại vi (máy in, máy quét và các thiết bị số hóa, thiết bị lưu trữ dữ liệu di động);

c) Đường truyền dữ liệu, đường truyền Internet;

d) Mạng nội bộ (LAN), mạng diện rộng (WAN) và thiết bị kết nối mạng, thiết bị bảo mật, thiết bị phụ trợ;

đ) Thiết bị CNTT kết nối mạng trong các cơ quan, đơn vị.

2. Hệ thống thông tin, phần mềm, ứng dụng và cơ sở dữ liệu:

a) Hệ thống thông tin, cơ sở dữ liệu dùng chung (hệ thống thư điện tử, hệ thống phần mềm một cửa và Cổng dịch vụ công, hệ thống phần mềm văn phòng điện tử eGov, phần mềm Họp không giấy, phần mềm hỏi đáp trực tuyến, phần mềm đánh giá các chỉ số);

b) Cổng thông tin điện tử của tỉnh và Cổng/trang thông tin điện tử của các cơ quan, đơn vị;

c) Hệ thống thông tin nghiệp vụ và các cơ sở dữ liệu chuyên ngành.

3. Thông tin, dữ liệu trao đổi, truyền tải, xử lý và lưu trữ trên Phòng tích hợp dữ liệu và hạ tầng kỹ thuật của tỉnh.

Điều 5. Nguyên tắc bảo đảm ATTT mạng

1. Bảo đảm ATTT mạng là yêu cầu bắt buộc, có tính xuyên suốt và phải

thường xuyên, liên tục được nâng cao, cải tiến trong quá trình:

a) Thu thập, tạo lập, xử lý, truyền tải, lưu trữ và sử dụng thông tin, dữ liệu;

b) Thiết kế, xây dựng, vận hành, nâng cấp hoặc hủy bỏ hệ thống thông tin.

2. Cơ quan, tổ chức, cá nhân có trách nhiệm bảo đảm ATTT mạng. Hoạt động ATTT mạng của cơ quan, tổ chức, cá nhân phải đúng quy định của pháp luật, bảo đảm quốc phòng, an ninh quốc gia, bí mật nhà nước.

3. Công tác đảm bảo ATTT mạng phải được thực hiện trên cơ sở có sự phối hợp chặt chẽ giữa các cơ quan, đơn vị và cá nhân.

4. Xử lý sự cố ATTT phải phù hợp với trách nhiệm, quyền hạn và bảo đảm lợi ích hợp pháp của cơ quan, đơn vị và theo quy định của pháp luật.

5. Các cơ quan, đơn vị phải bố trí máy vi tính riêng, nghiêm cấm sử dụng máy tính kết nối Internet và các thiết bị di động thông minh để soạn thảo văn bản, lưu giữ thông tin có nội dung mật theo quy định. Các thiết bị viễn thông, máy tính được sử dụng để lưu giữ và truyền thông tin bí mật nhà nước phải được chứng nhận của cơ quan chức năng kiểm tra, kiểm định trước khi đưa vào sử dụng.

6. Phải có phương án tổ chức sao lưu dữ liệu dự phòng cho mọi dữ liệu quan trọng của tỉnh, của cơ quan, đơn vị mình. Lãnh đạo cơ quan, đơn vị phải chịu trách nhiệm nếu để xảy ra mất mát dữ liệu do không tiến hành sao lưu dự phòng.

7. Để phục vụ hoạt động theo dõi, giám sát, phân tích và điều tra, các cơ quan, đơn vị phải thực hiện việc lưu trữ nhật ký của các hệ thống tại các máy chủ (của hệ điều hành và các phần mềm ứng dụng) trong thời gian ít nhất là 30 ngày.

8. Các thiết bị viễn thông, máy tính có chứa tài liệu của cơ quan nhà nước khi đưa đi công tác nước ngoài phải thực hiện theo quy định của pháp luật về bảo vệ bí mật nhà nước.

Điều 6. Các hành vi bị nghiêm cấm

Theo quy định tại Điều 7 Luật An toàn thông tin mạng.

Chương II

NỘI DUNG BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 7. Bảo đảm ATTT cho Phòng tích hợp dữ liệu của đơn vị

1. Trung tâm Y tế huyện Phù Mỹ có trách nhiệm đảm bảo an toàn cho Phòng tích hợp dữ liệu của đơn vị, bao gồm các nội dung sau:

a) Xây dựng phương án đảm bảo ATTT cho dữ liệu của cơ quan, đơn vị đặt tại Phòng tích hợp dữ liệu nhưng phải đảm bảo thuận lợi cho việc truy xuất

và sử dụng các dữ liệu này;

b) Xây dựng Quy chế quản lý vận hành Phòng tích hợp dữ liệu của phòng;

c) Xây dựng quy trình ứng phó các sự cố có thể xảy ra tại phòng tích hợp dữ liệu của đơn vị;

d) Đảm bảo các điều kiện về hạ tầng kỹ thuật. ATTT đối với hệ thống máy chủ, thiết bị kết nối mạng đặt tại phòng tích hợp dữ liệu của đơn vị.

2. Các cơ quan, đơn vị đặt dữ liệu hoặc kết nối vào phòng tích hợp dữ liệu của đơn vị phải tuân thủ các chính sách ATTT liên quan đến việc kết nối vào phòng tích hợp dữ liệu của đơn vị do Sở Thông tin và Truyền thông hướng dẫn; tự bảo vệ hệ thống đầu cuối của mình và phải chịu trách nhiệm nếu để tin tặc kiểm soát máy tính và tấn công ngược vào phòng tích hợp dữ liệu của đơn vị. Các hệ thống thông tin trước khi cài đặt trên phòng tích hợp dữ liệu của đơn vị phải được kiểm tra, xác nhận về tính an toàn, bảo mật.

3. Bảo đảm ATTT mức vật lý là việc bảo vệ hệ thống hạ tầng kỹ thuật, phần mềm, ứng dụng và cơ sở dữ liệu khỏi các mối nguy hiểm vật lý (như: cháy, nổ; nhiệt độ, độ ẩm ngoài mức cho phép; thiên tai; mất điện; tác động cơ học) có thể gây ảnh hưởng đến hoạt động hệ thống.

4. Các biện pháp cơ bản bảo đảm ATTT mức vật lý bao gồm:

a) Quản lý phòng tích hợp dữ liệu của đơn vị:

Các thiết bị kết nối mạng, thiết bị bảo mật quan trọng như tường lửa, thiết bị định tuyến, hệ thống máy chủ, hệ thống lưu trữ SAN, NAS phải được đặt trong phòng tích hợp dữ liệu của đơn vị.

Phòng tích hợp dữ liệu của đơn vị phải được thiết lập cơ chế bảo vệ, theo dõi, phát hiện xâm nhập và biện pháp kiểm soát truy nhập, kết nối vật lý phù hợp đối với từng khu vực: máy chủ và hệ thống lưu trữ; từ mạng và đầu nối; thiết bị nguồn điện và dự phòng điện khẩn cấp; vận hành, kiểm soát, quản trị hệ thống.

Quá trình vào, ra hoặc bàn giao ca trực Phòng tích hợp dữ liệu phải được ghi nhận vào nhật ký quản lý Phòng tích hợp dữ liệu. Chỉ những cá nhân có quyền, nhiệm vụ theo quy định có thủ trưởng cơ quan, đơn vị mới được phép vào Phòng tích hợp dữ liệu của đơn vị.

Có phương án, kế hoạch phòng, chống và khắc phục sự cố ngập dột nước, sét, tĩnh điện, cháy nổ; áp dụng các quy chuẩn kỹ thuật về an toàn kỹ thuật nhiệt, độ ẩm, ánh sáng cho các thiết bị tính toán, lưu trữ; bảo đảm điều kiện hoạt động ổn định cho các hệ thống hỗ trợ như máy điều hòa nhiệt độ, nguồn cấp điện, dây dẫn;

Phòng tích hợp dữ liệu của đơn vị được trang bị hệ thống lưu điện đủ công suất và duy trì thời gian hoạt động của các máy chủ ít nhất 15 phút khi có sự cố mất điện.

b) Thiết lập cơ chế dự phòng đối với các thiết bị hạ tầng kỹ thuật quan trọng; có kế hoạch kiểm tra, bảo dưỡng định kỳ và duy trì thông số kỹ thuật các thiết bị này hoặc có phương án sửa chữa, thay thế đáp ứng yêu cầu về độ sẵn sàng trong suốt thời gian lắp đặt, sử dụng;

c) Các đường truyền dữ liệu, đường truyền Internet và hệ thống dây dẫn các mạng WAN, LAN phải được lắp đặt trong ống, máng che đậy kín, hạn chế khả năng tiếp cận trái phép. Ngắt kết nối cổng Ethernet không sử dụng, đặc biệt là ở khu vực làm việc chung của các cơ quan, đơn vị;

d) Cá nhân sử dụng thiết bị lưu trữ dữ liệu di động để lưu trữ thông tin, dữ liệu của cơ quan, đơn vị mình có trách nhiệm bảo vệ thiết bị này và thông tin lưu trên thiết bị, tránh làm mất hoặc lộ, lọt thông tin, dữ liệu;

đ) Thiết bị tính toán có bộ phận lưu trữ hoặc thiết bị lưu trữ khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài cơ quan, đơn vị hoặc ngừng sử dụng phải được tháo bộ phận lưu trữ khỏi thiết bị hoặc xóa thông tin, dữ liệu lưu trữ trên thiết bị (trừ trường hợp để khôi phục dữ liệu). Khi thanh lý thiết bị thì phải xóa nội dung lưu trữ bằng phần mềm hoặc thiết bị hủy dữ liệu chuyên dụng hay phá hủy vật lý.

3. Cơ quan, đơn vị có trách nhiệm xây dựng quy trình bảo dưỡng, bảo trì và hướng dẫn cách sử dụng, quản lý, vận hành hệ thống hạ tầng kỹ thuật của mình; chỉ định bộ phận chuyên trách về CNTT thực hiện quản lý, vận hành và định kỳ kiểm tra, sửa chữa, bảo trì thiết bị (bao gồm thiết bị đang hoạt động và thiết bị dự phòng).

4. Bảo đảm an toàn cho máy tính, thiết bị công nghệ thông tin và an toàn dữ liệu

Cá nhân sử dụng máy tính để xử lý công việc tuân thủ các quy định sau:

a) Chỉ cài đặt phần mềm hợp lệ (phần mềm có bản quyền thương mại, phần mềm nội bộ được đầu tư hoặc phần mềm mã nguồn mở có nguồn gốc rõ ràng) và thuộc danh mục phần mềm được phép sử dụng do cơ quan, đơn vị có thẩm quyền ban hành (nếu có) trên máy tính được cơ quan, đơn vị cấp cho mình:

b) Cài đặt phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm; thực hiện kiểm tra, rà quét phần mềm trước khi sao chép, mở các tập tin hoặc trước khi kết nối các thiết bị lưu trữ dữ liệu di động với máy tính của mình; trước khi cài đặt, kết nối phần mềm ứng dụng vào hạ tầng mạng nội bộ, hạ tầng Phòng tích hợp dữ liệu cần thực hiện hiện kiểm tra để phòng, tránh phần mềm độc hại;

c) Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy tính (máy chạy chậm bất thường, cảnh báo từ phần mềm phòng, chống phần mềm độc hại, mất dữ liệu,...), phải ngắt kết nối giữa máy với mạng nội bộ và báo trực tiếp cho bộ phận chuyên trách về CNTT để được xử lý kịp thời;

d) Chỉ truy nhập vào các trang/cổng thông tin điện tử, ứng dụng trực tuyến tin cậy và các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình; sử dụng những trình duyệt an toàn; không truy nhập, mở các trang tin, thư điện tử không rõ nguồn gốc: không sử dụng tính năng lưu mật khẩu tự động hoặc đăng nhập tự động;

đ) Máy tính cá nhân phải được cài đặt mật khẩu và thực hiện thao tác khóa máy tính (sử dụng tính năng có sẵn trên máy tính) khi rời khỏi nơi đặt máy tính; tắt máy tính khi rời khỏi cơ quan;

e) Phải sử dụng hộp thư điện tử công vụ của cơ quan có tên miền: @ttytan.gov.vn hoặc hộp thư điện tử có tên miền đặc thù theo quy định của ngành nhưng phải đảm bảo tính an toàn, bảo mật khi trao đổi trên môi trường mạng trong quá trình thực hiện nhiệm vụ công vụ;

g) Báo cáo và phải được thủ trưởng cơ quan, đơn vị đồng ý, cho phép trước khi mang máy tính, thiết bị CNTT có kết nối mạng thuộc sở hữu riêng đến nơi làm việc và kết nối với mạng nội bộ để thực hiện xử lý công việc. Trong trường hợp này, cá nhân phải tuân thủ đầy đủ các quy định tại các Điểm a, b, c, d, đ, e, g của Khoản này và chịu sự giám sát của bộ phận chuyên trách về CNTT của cơ quan, đơn vị.

5. Tài khoản truy nhập

a) Cá nhân sử dụng hệ thống thông tin được cấp và sử dụng tài khoản truy nhập với định danh duy nhất gắn với cá nhân đó;

b) Trường hợp cá nhân thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ hưu, trong vòng không quá 05 ngày làm việc, cơ quan, đơn vị quản lý cá nhân đó phải thông báo cơ quan, đơn vị chủ quản hệ thống thông tin để điều chỉnh, thu hồi, hủy bỏ các quyền sử dụng đối với hệ thống thông tin; tài khoản quản trị hệ thống (mạng, hệ điều hành, thiết bị kết nối mạng, phần mềm, ứng dụng, cơ sở dữ liệu) phải tách biệt với tài khoản truy nhập của người sử dụng thông thường. Tài khoản quản trị hệ thống phải được giao đích danh cá nhân làm công tác quản trị. Hạn chế dùng chung tài khoản quản trị;

c) Có trách nhiệm bảo mật tài khoản truy nhập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác. Đặt mật khẩu với độ an toàn cao (có chữ thường, có chữ in hoa, có số và ký tự đặc biệt như @, #, !) và khuyến khích thay đổi mật khẩu ít nhất 03 tháng/lần; các tài khoản đăng nhập các hệ thống phải được đăng xuất khi không sử dụng; thường xuyên xóa các biểu mẫu, mật khẩu, bộ nhớ cache và cookie trong trình duyệt trên máy tính;

d) Tạm dừng quyền sử dụng đối với tài khoản đã được đăng ký trên hệ thống nhưng không làm việc trong hệ thống từ 30 ngày trở lên.

Điều 8. Bảo đảm ATTT đối với mạng máy tính

1. Hệ thống mạng nội bộ (LAN) phải được thiết kế phân vùng theo chức năng cơ bản, bao gồm: vùng mạng người dùng; vùng mạng kết nối hệ thống ra

bên ngoài Internet và các mạng khác; vùng mạng máy chủ công cộng; vùng mạng máy chủ nội bộ; vùng mạng máy chủ quản trị. Dữ liệu trao đổi giữa các vùng mạng phải được quản lý giám sát bởi các hệ thống các thiết bị mạng, thiết bị bảo mật.

Căn cứ điều kiện, yêu cầu thực tế về bảo mật dữ liệu, cơ quan, đơn vị là chủ quản hệ thống mạng nội bộ chủ động triển khai xây dựng mô hình, giải pháp an toàn bảo mật, bao gồm các biện pháp kỹ thuật như sau:

a) Bước 1: Kiểm soát truy nhập từ bên ngoài mạng *(sử dụng các giao thức mạng có hỗ trợ chức năng mã hóa thông tin như SSH, SSL/TLS, VPN)*;

b) Bước 2: Kiểm soát truy nhập từ bên trong mạng (quản lý các thiết bị đầu cuối, máy tính người sử dụng kết nối vào hệ thống mạng; giám sát, phát hiện và ngăn chặn truy nhập từ bên trong mạng đến các địa chỉ Internet bị cấm truy nhập);

c) Bước 3: Phòng, chống xâm nhập và phần mềm độc hại, bảo vệ các vùng mạng máy chủ công cộng, máy chủ nội bộ, máy chủ cơ sở dữ liệu và vùng mạng nội bộ; có khả năng tự động cập nhật thời gian thực cơ sở dữ liệu, dấu hiệu phát hiện tấn công. Vô hiệu hóa tất cả các dịch vụ không cần thiết tại từng vùng mạng;

d) Bước 4: Cấu hình chức năng xác thực trên các thiết bị kết nối mạng để xác thực người sử dụng quản trị thiết bị trực tiếp hoặc từ xa;

đ) Bước 5: Mạng không dây phải có cơ chế bảo toàn tính toàn vẹn và bí mật của thông tin được truyền đư trên môi trường mạng, có hướng dẫn bảo đảm ATTT dành cho các thiết bị đầu cuối khi kết nối vào mạng; được thiết lập các tham số: tên, nhận dạng dịch vụ (SSID), mật khẩu, cấp phép truy nhập đối với địa chỉ vật lý (MAC address), mã hóa dữ liệu. Thường xuyên thay đổi mật khẩu. Các điểm truy nhập không dây phải được bảo vệ, tránh bị tiếp cận trái phép;

e) Bước 6: Hệ thống máy chủ phải có chức năng tự động cập nhật bản ghi nhật ký hệ thống trong khoảng thời gian nhất định (tối thiểu là 03 tháng), lưu trữ thông tin kết nối mạng, quá trình đăng nhập vào máy chủ, các thao tác cấu hình hệ thống, lỗi phát sinh trong quá trình hoạt động và các thông tin liên quan về ATTT để phục vụ công tác khắc phục sự cố và điều tra về ATTT khi xảy ra. Xóa sạch thông tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng.

2. Cơ quan, đơn vị tham gia kết nối, sử dụng hệ thống mạng diện rộng (WAN), mạng truyền số liệu chuyên dùng của tỉnh có trách nhiệm:

a) Bảo đảm ATTT đối với hệ thống mạng nội bộ và các thiết bị của mình khi thực hiện kết nối vào hệ thống mạng diện rộng, mạng truyền số liệu chuyên dùng; thông báo sự cố hoặc các hành vi phá hoại, xâm nhập về Sở Thông tin và Truyền thông để xử lý;

b) Phối hợp với Sở Thông tin và Truyền thông rà soát đánh giá tính hợp lệ

cấu hình địa chỉ IP kết nối mạng diện rộng, mạng truyền số liệu chuyên dùng trong quá trình vận hành và sử dụng các hệ thống thông tin, máy chủ, thiết bị CNTT của mình có kết nối với hệ thống mạng diện rộng;

c) Định kỳ sao lưu thông tin, dữ liệu dùng chung lưu trữ trên mạng diện rộng;

d) Không tiết lộ phương thức (tên đăng ký, mật khẩu, tiện ích, tệp hỗ trợ và các cách thức khác) để truy nhập vào hệ thống mạng diện rộng, mạng Truyền số liệu chuyên dùng cho tổ chức, cá nhân khác; không được tìm cách truy nhập dưới bất cứ hình thức nào vào các khu vực không được phép truy nhập.

3. Cơ quan, đơn vị phải áp dụng các biện pháp kỹ thuật cần thiết bảo đảm ATTT trong hoạt động kết nối Internet, tối thiểu đáp ứng các yêu cầu sau;

a) Có hệ thống tường lửa và hệ thống bảo vệ kiểm soát truy nhập Internet, đáp ứng nhu cầu kết nối đồng thời, hỗ trợ các công nghệ mạng riêng ảo thông dụng và có phần cứng mã hóa tích hợp để tăng tốc độ mã hóa dữ liệu, cung cấp đầy đủ các cơ chế bảo mật cơ bản như NAT, PAT, quản lý luồng dữ liệu ra , vào và có khả năng bảo vệ hệ thống trước các loại tấn công từ chối dịch vụ (DDoS);

b) Lọc bỏ, không cho phép truy nhập các trang tin có nghi ngờ chứa mã độc hoặc các nội dung không phù hợp;

c) Không mở trang tin hoặc ứng dụng Internet trên máy tính chứa dữ liệu quan trọng hoặc có khả năng tiếp cận các dữ liệu, ứng dụng quan trọng; chỉ thiết lập kết nối Internet cho các máy chủ và thiết bị CNTT cần phải có giao tiếp với Internet (các máy chủ, thiết bị cung cấp giao diện ra Internet của trang tin điện tử, dịch vụ công, thư điện tử; thiết bị cập nhật bản vá hệ điều hành, mẫu mã độc, mẫu điểm yếu, mẫu tấn công).

Điều 9. Kiểm tra, khắc phục sự cố ATTT

1. Cơ quan, đơn vị chủ quản hệ thống thông tin có trách nhiệm phối hợp với các cơ quan, đơn vị chuyên trách về CNTT, ATTT của tỉnh:

a) Rà soát, đánh giá và xác định các sự cố ATTT, các rủi ro ATTT có thể xảy ra với từng thành phần hệ thống thông tin trong phạm vi quản lý của mình. Trên cơ sở đó, xây dựng và phê duyệt các phương án ứng cứu, xử lý sự cố phù hợp với các rủi ro ATTT có thể xảy ra;

b) Chuẩn bị sẵn sàng các biện pháp, phương tiện kỹ thuật để phục vụ cho triển khai các phương án ứng cứu đã được xây dựng:

c) Xây dựng và ban hành các hướng dẫn, quy trình xử lý sự cố ATTT đối với từng đối tượng người sử dụng cụ thể trong hệ thống thông tin theo hướng dẫn của Sở Thông tin và Truyền thông;

d) Thông báo công khai các phương án liên lạc với bộ phận xử lý sự cố cho toàn bộ cá nhân liên quan hệ thống thông tin đang quản lý;

đ) Thường xuyên kiểm tra, rà soát tính sẵn sàng của các phương án ứng cứu sự cố; thực hiện đúng các hướng dẫn, quy trình xử lý sự cố ATTT.

2. Khi có sự cố hoặc nguy cơ mất ATTT, thủ trưởng cơ quan, đơn vị thực hiện:

a) Chỉ đạo xác định nguyên nhân sự cố, có biện pháp khắc phục kịp thời, hạn chế thiệt hại;

b) Trường hợp gặp sự cố nghiêm trọng ở mức độ cao, khẩn cấp (hệ thống bị gián đoạn dịch vụ; dữ liệu tuyệt mật hoặc bí mật nhà nước có khả năng bị tiết lộ; dữ liệu quan trọng của hệ thống không bảo đảm tính toàn vẹn và không có khả năng khôi phục được; hệ thống bị mất quyền điều khiển) hoặc chủ quản hệ thống không đủ khả năng tự kiểm soát, xử lý được sự cố thì phải phối hợp chặt chẽ với Đội ứng cứu sự cố ATTT mạng của tỉnh và cung cấp đầy đủ thông tin sự cố để được hướng dẫn, hỗ trợ cụ thể;

c) Chuẩn bị nội dung báo cáo sự cố, bao gồm:

Tên, địa chỉ Đơn vị vận hành hệ thống thông tin; chủ quản hệ thống thông tin; hệ thống thông tin bị sự cố; thời điểm phát hiện sự cố;

Đầu mối liên lạc về sự cố của đơn vị vận hành hệ thống bị sự cố: Tên, chức vụ, điện thoại, thư điện tử;

Mô tả về sự cố: Loại sự cố, hiện tượng, đánh giá sơ bộ mức độ nguy hại, mức độ lây lan, tác động của sự cố đến hoạt động bình thường của tổ chức;

Đơn vị cung cấp dịch vụ hạ tầng kỹ thuật;

Liệt kê các biện pháp đã triển khai hoặc dự kiến triển khai để xử lý khắc phục sự cố;

Các tổ chức, doanh nghiệp đang hỗ trợ ứng cứu, xử lý và kết quả xử lý sự cố tính đến thời điểm báo cáo;

Kết quả ứng cứu sự cố ban đầu;

Kiến nghị đề xuất hướng ứng cứu xử lý sự cố (nếu có);

Bản cập nhật mới nhất của tài liệu mô tả các thành phần hệ thống thông tin, bao gồm: các vùng mạng chức năng; hệ thống thiết bị mạng, thiết bị bảo mật; hệ thống máy chủ hệ thống; hệ thống máy chủ ứng dụng; dịch vụ và các thành phần khác trong hệ thống thông tin (trong trường hợp sự cố có khả năng xảy ra trên diện rộng hoặc gây ra các ảnh hưởng dây chuyền, làm tổn hại cho các hệ thống thông tin quan trọng khác).

Điều 10. Giám sát an toàn hệ thống thông tin mạng

1. Đối với các cơ quan, đơn vị:

Tổ chức thực hiện việc giám sát an toàn hệ thống thông tin của cơ quan, đơn vị trực tiếp quản lý. Nội dung và đối tượng giám sát thực hiện theo quy định

tại các khoản 1, khoản 2 Điều 24 của Luật ATTT mạng; thực hiện việc lưu trữ nhật ký tình trạng hoạt động của các hệ thống thông tin tại các máy chủ trong thời gian ít nhất là 30 ngày để phục vụ các công tác đảm bảo ATTT mạng.

2. Đối với các doanh nghiệp cung cấp các dịch vụ viễn thông, CNTT, Internet có trách nhiệm thực hiện theo quy định tại khoản 3 Điều 24 của Luật ATTT mạng.

(*)Trên cơ sở quy chế này và hướng dẫn của Bộ, ngành Trung ương, các sở, ban, ngành tỉnh, Trung tâm y tế Huyện Phù Mỹ ban hành quy chế bảo đảm ATTT nội bộ tại cơ quan quy định rõ các vấn đề cơ bản sau:

1. Phân công cụ thể cán bộ, công chức chuyên trách CNTT, số điện thoại liên hệ khi có sự cố về ATTT.

2. Phân công cán bộ, công chức chịu trách nhiệm quản lý máy tính để dự thảo các văn bản, tài liệu có tính mật; việc sử dụng và vận hành máy tính này, đảm bảo tuân thủ các quy định của pháp luật về bảo mật và ATTT.

3. Thiết lập quy tắc vào ra, quản lý phòng máy chủ; quy tắc cài đặt phần mềm lên máy chủ, máy tính trạm.

4. Quy tắc phân loại và quản lý mức độ ưu tiên đối với các tài nguyên của hệ thống thông tin (phần mềm, dữ liệu, trang thiết bị CNTT).

5. Kiểm tra, rà soát và khắc phục sự cố an toàn của hệ thống thông tin sử dụng các biện pháp trong Điều 9 của Quy chế này.

6. Quy tắc quản lý bảo đảm an toàn hệ thống thông tin tại đơn vị; đảm bảo tính toàn vẹn, tính tin cậy, tính thống nhất và tính sẵn sàng của dữ liệu trong quản lý và vận hành trao đổi thông tin.

7. Quy trình xử lý các sự cố ảnh hưởng đến an toàn hệ thống tại đơn vị.

8. Chế độ báo cáo tổng hợp tình hình an toàn của hệ thống thông tin.

Điều 11. Quy trình phối hợp ứng cứu sự cố mạng bảo đảm ATTT

1. Quy trình xử lý khẩn cấp:

Khi phát hiện hệ thống có nguy cơ mất ATTT như: hệ thống hoạt động chậm bất thường, không truy cập được hệ thống ứng dụng, nội dung cổng (trang) thông tin điện tử hoặc giao diện ứng dụng bị thay đổi, các sự cố khác có liên quan thực hiện các bước cơ bản như sau:

a) Bước 1: Ngắt kết nối hệ thống máy chủ ra khỏi hệ thống mạng, báo cáo sự cố đến Thủ trưởng cơ quan, đơn vị;

b) Bước 2: Sao chép nhật ký truy cập của người dùng (logfile) và toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ (phục vụ cho công tác phân tích);

c) Bước 3: Khôi phục lại hệ thống, hoặc sử dụng hệ thống dự phòng và chuyển dữ liệu sao lưu dự phòng (backup) mới nhất để hệ thống hoạt động;

d) Bước 4: Tổng hợp, báo cáo sự cố và nội dung khắc phục gửi về Đội ứng cứu để tổng hợp.

2. Nguyên tắc phối hợp trong ứng cứu sự cố:

a) Đơn vị vận hành hệ thống thông tin:

Thực hiện các bước khắc phục sự cố theo Khoản 1 điều này.

Các sự cố vượt quá khả năng xử lý, đơn vị thông báo đến Đội ứng cứu để hỗ trợ khắc phục và thực hiện báo cáo sự cố mạng.

b) Đội ứng cứu:

Tiếp nhận thông tin, báo cáo sự cố mất an toàn thông tin của đơn vị. Phản hồi đến email cần hỗ trợ theo 03 bước: Tiếp nhận, Hướng xử lý, đóng xử lý. Việc xử lý lỗi được thực hiện ngay khi nhận được email yêu cầu.

Phản hồi cho đơn vị, cá nhân gửi thông báo, báo cáo ban đầu ngay sau khi nhận được để xác nhận về việc đã nhận được thông báo, báo cáo sự cố.

Thẩm tra, xác minh và phân loại sự cố an toàn thông tin mạng để lựa chọn phương án ứng cứu phù hợp hoặc đề xuất với Ban chỉ đạo hướng giải quyết trong trường hợp vượt thẩm quyền.

Chủ động hỗ trợ ngay đơn vị cần ứng cứu, xử lý sự cố trong khả năng và trách nhiệm của mình, cử cán bộ kỹ thuật của Đội có mặt tại đơn vị báo sự cố để phối hợp, hướng dẫn, ghi nhận giải quyết sự cố, trong trường hợp sự cố phức tạp, nguy cơ cao về ATTT mà không thể hướng dẫn, trao đổi qua điện thoại, email với đơn vị bị sự cố.

Giám sát diễn biến tình hình ứng cứu sự cố và báo cáo Ban chỉ đạo, đề xuất, xin ý kiến chỉ đạo trong trường hợp không thuộc thẩm quyền, phạm vi trách nhiệm hoặc vượt khả năng xử lý của mình.

Chương III

TỔ CHỨC THỰC HIỆN

Điều 12. Trách nhiệm của tổ chức, cá nhân bên ngoài khi tham gia sử dụng hệ thống thông tin của cơ quan nhà nước, để giao tiếp, cung cấp và trao đổi thông tin số với cơ quan nhà nước

1. Nghiêm chỉnh thi hành quy chế này và các quy định khác của pháp luật về bảo đảm ATTT mạng.

2. Khi phát hiện sự cố ảnh hưởng đến an toàn hệ thống thông tin, phải thông báo ngay với cơ quan nhà nước, nơi tổ chức, cá nhân đang thực hiện giao tiếp.

3. Các tổ chức, cá nhân tham gia vào quá trình ứng dụng CNTT trên địa bàn tỉnh, chịu sự thanh tra, kiểm tra của các cơ quan nhà nước có thẩm quyền về lĩnh vực ATTT.

4. Nghiêm chỉnh thi hành quy chế này và các quy định khác của pháp luật về bảo đảm ATTT.

5. Khi phát hiện sự cố ảnh hưởng đến an toàn hệ thống thông tin, phải thông báo ngay đến cán bộ, công chức chuyên trách CNTT của đơn vị.

3. Các thông tin, tài liệu, văn bản có tính mật theo quy định, phải dự thảo, lưu trữ đúng theo quy định về bảo mật và ATTT.

6. Cán bộ, công chức chuyên trách CNTT:

a) Theo nhiệm vụ được Thủ trưởng cơ quan, đơn vị phân công, chịu trách nhiệm tham mưu chuyên môn và vận hành đảm bảo an toàn hệ thống thông tin tại cơ quan, đơn vị;

b) Hướng dẫn, hỗ trợ người dùng tại cơ quan, đơn vị giải pháp phòng, chống vi rút, mã độc máy tính. Thực hiện việc đánh giá, báo cáo các rủi ro và mức độ các rủi ro ảnh hưởng đến hoạt động hệ thống thông tin của đơn vị, các giải pháp cơ bản khắc phục các rủi ro:

c) Phối hợp với các cá nhân, tổ chức có liên quan trong việc kiểm tra, phát hiện, phòng ngừa, đấu tranh, ngăn chặn xâm phạm ATTT; tham gia khắc phục các sự cố mất ATTT.

Điều 13. Trách nhiệm của các cơ quan, đơn vị

1. Đảm bảo an toàn thông tin mạng theo quy định hiện hành của Chính phủ. Bộ Thông tin và Truyền thông. Quy chế này và các quy chế nội bộ khác.

2. Tuân thủ và bảo đảm ATTT trong ứng dụng CNTT, đảm bảo an toàn thông tin mạng nội bộ của cơ quan, đơn vị theo hướng dẫn của Sở Thông tin và Truyền thông theo quy định của quy chế này và các quy định khác của pháp luật có liên quan.

3. Tuyên truyền, phổ biến quy chế này và các quy định khác của pháp luật có liên quan về ATTT trong phạm vi trách nhiệm và quyền hạn của từng cơ quan đơn vị.

5. Xác định và trình cấp có thẩm quyền phê duyệt cấp độ hệ thống thông tin của cơ quan, đơn vị.

6. Khi được kiểm tra công tác đảm bảo an toàn thông tin mạng tại cơ quan, đơn vị cử cán bộ có chuyên môn về CNTT tham gia đoàn kiểm tra; phối hợp với đoàn kiểm tra xây dựng các tiêu chí và quy trình kỹ thuật kiểm tra công tác đảm bảo ATTT.

7. Xây dựng Quy chế đảm bảo ATTT nội bộ tại cơ quan, đơn vị theo quy định tại Điều 8 của Quy chế này.

Điều 14. Trách nhiệm thi hành

1. Trung tâm y tế huyện Phù Mỹ và các đơn vị có liên quan triển khai

thực hiện Quy chế này.

2. Các văn bản quy phạm pháp luật dẫn chiếu để áp dụng tại Quy chế này được sửa đổi, bổ sung hoặc thay thế bằng văn bản mới thì áp dụng theo các văn bản sửa đổi, bổ sung hoặc thay thế.

3. Trong quá trình thực hiện, nếu có phát sinh khó khăn, vướng mắc, các bộ phận trực thuộc kịp thời báo cáo về Trung tâm Y tế Phù Mỹ để TTYT báo cáo về Sở Thông tin và Truyền thông tổng hợp để trình UBND tỉnh xem xét, quyết định./.