UBND TỈNH QUẢNG NGÃI
SỞ Y TẾ

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

Số: 3887 /QĐ-SYT

Quảng Ngãi, ngày 11 tháng 11 năm 2015

QUYẾT ĐỊNH
Ban hành Quy chế bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin trong toàn ngành Y tế tỉnh Quảng Ngãi

Căn cứ Luật Giao dịch điện tử ngày 29 tháng 11 năm 2005;

Căn cứ Luật Công nghệ thông tin ngày 29 tháng 6 năm 2006;

Căn cứ Nghị định số 63/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ quy định xử phạt vi phạm hành chính trong lĩnh vực công nghệ thông tin;

Căn cứ 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;

Căn cứ Nghị định số 72/2013/NĐ-CP ngày 15 tháng 7 năm 2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng;

Căn cứ Chỉ thị số 897/CT-TTg ngày 10 tháng 6 năm 2011 của Thủ tướng Chính phủ về việc triển khai các hoạt động đảm bảo an toàn thông tin số;

Căn cứ Thông tư số 22/2013/TT-BTTTT ngày 23 tháng 12 năm 2013 của Bộ Thông tin và Truyền thông về công bố danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước;

Căn cứ Thông tư số 25/2014/TT-BTTTT ngày 30 tháng 12 năm 2014 của Bộ Thông tin và Truyền thông về quy định về triển khai các hệ thống thông tin có quy mô và phạm vi từ Trung ương đến địa phương;

Căn cứ Quyết định số 44/2012/QĐ-UBND ngày 06/12/2012 của UBND tỉnh Quảng Ngãi về Ban hành Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan, đơn vị quản lý nhà nước tỉnh Quảng Ngãi;

Căn cứ Quyết định 213/QĐ-UBND ngày 06/08/2008 của UBND tỉnh Quảng Ngãi về ban hành Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức bộ máy của Sở Y tế tỉnh Quảng Ngãi;

Theo đề nghị của Chánh Văn phòng Sở Y tế,

QUYẾT ĐỊNH:

Điều 1: Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin trong toàn ngành Y tế tỉnh Quảng Ngãi.

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

Điều 3: Chánh Văn phòng, Trưởng các phòng chức năng thuộc cơ quan Sở Y tế; Thủ trưởng các đơn vị trực thuộc chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- UBND tỉnh (b/c);
- Sở TT & TT (b/c);
- Lưu: VT.

GIÁM ĐỐC

SỞ Y TẾ

Nguyễn Tấn Đức

UBND TỈNH QUẢNG NGÃI
SỞ Y TẾ

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

QUY CHẾ

Quy chế bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin trong toàn ngành Y tế tỉnh Quảng Ngãi

(Ban hành kèm theo Quyết định số 3887/QĐ-SYT ngày 11 tháng 11 năm 2015 của Giám đốc Sở Y tế Quảng Ngãi)

CHƯƠNG I
NHỮNG QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định chi tiết nội dung đảm bảo an toàn, an ninh thông tin (ANTT) trong hoạt động công nghệ thông tin tại cơ quan Sở Y tế và các đơn vị trực thuộc Sở Y tế.

Điều 2. Đối tượng áp dụng

Quy chế này áp dụng đối với cán bộ, công chức, viên chức đang làm việc tại cơ quan Sở Y tế và các đơn vị trực thuộc Sở Y tế.

Điều 3. Mục đích đảm bảo an toàn, an ninh thông tin

1. Bảo vệ toàn diện, ngăn chặn các mối đe dọa, giảm thiểu các rủi ro do môi trường bị gián đoạn, lỗi của con người hoặc máy, các cuộc tấn công có mục đích làm mất an toàn thông tin; bảo đảm an toàn, ANTT cho các đơn vị trên môi trường mạng.

2. Bảo vệ chống lại hành vi vô tình hay cố ý thay đổi trái phép, phá hủy, làm chậm trễ, trộm cắp, truy cập (khi không được quyền) gây thiệt hại cho hệ thống, dữ liệu, ứng dụng, thiết bị và viễn thông.

3. Việc nghiên cứu, ứng dụng và phát triển CNTT của các đơn vị phải bảo đảm tính bảo mật, an toàn, ANTT, hợp lý và hiệu quả.

4. Các đơn vị tự xây dựng quy định nội bộ về đảm bảo an toàn thông tin, ANTT; bố trí cán bộ chuyên trách, phụ trách quản lý an toàn thông tin, ANTT; quy định quyền hạn, trách nhiệm của thủ trưởng đơn vị, các bộ phận liên quan trong đơn vị đối với công tác bảo đảm an toàn, ANTT trong đơn vị.

Điều 4. Giải thích từ ngữ

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

1. TCVN ISO/IEC 27001:2009 (ISO/IEC 27001:2005): CNTT - Hệ thống quản lý an toàn thông tin - Các yêu cầu.

2. TCVN ISO/IEC 27002:2011 (ISO/IEC 27002:2005): CNTT - các kỹ thuật an toàn - quy tắc thực hành quản lý an toàn thông tin.

3. Tính bảo mật: Bảo đảm thông tin chỉ có thể được truy cập bởi những người được cấp quyền sử dụng.

4. Tính sẵn sàng: Bảo đảm những người được cấp quyền có thể truy cập thông tin và các tài sản liên quan ngay khi có nhu cầu.

5. Tính toàn vẹn: Bảo vệ tính chính xác và tính đầy đủ của thông tin và các phương pháp xử lý thông tin.

6. Tài sản CNTT:

a) Tài sản vật lý: Bao gồm các trang thiết bị phần cứng máy tính, thiết bị ngoại vi, phương tiện truyền thông và các thiết bị phục vụ cho hoạt động trong hệ thống CNTT của đơn vị.

b) Tài sản thông tin: các dữ liệu, thông tin ở dạng số hoặc tài liệu văn bản giấy, phương tiện lưu trữ khác.

c) Tài sản phần mềm: Các chương trình ứng dụng chuyên dụng, phần mềm hệ thống, công cụ phát triển và các công cụ hỗ trợ cho tác nghiệp tại đơn vị.

7. Hệ thống thông tin: Tập rời rạc các tài nguyên thông tin được tổ chức có cấu trúc cho việc thu thập, xử lý, chia sẻ, bảo trì, sử dụng phổ biến hay sắp xếp các dữ liệu, thông tin.

8. Kiểm soát ANTT: Tập hợp tất cả các hoạt động quản lý rủi ro, bao gồm cả chính sách, thủ tục, hướng dẫn, thực hành hoặc tổ chức cấu trúc, có thể được hành chính, quản lý, kỹ thuật, hoặc tính chất pháp lý nhằm bảo đảm an toàn, ANTT.

9. Nguồn lực CNTT: Tập hợp tất cả các thông tin và tài nguyên liên quan đến tổ chức bao gồm: nhân sự, thiết bị, tài chính và CNTT.

10. Rủi ro CNTT: Khả năng xảy ra tổn thất khi thực hiện các hoạt động liên quan đến hệ thống CNTT. Rủi ro CNTT liên quan đến quản lý, sử dụng phần cứng, phần mềm, truyền thông, giao diện hệ thống, vận hành và con người.

Điều 5. Các hành vi bị cấm

1. Cản trở, ngăn chặn, can thiệp trái phép việc truyền tải thông tin, xóa, thay đổi, làm sai lệch thông tin trên mạng, ảnh hưởng tới sự hoạt động bình thường của hệ thống thông tin hoặc khả năng truy cập hợp pháp của người sử dụng tới hệ thống thông tin.

2. Sử dụng trái phép tài khoản, mật khẩu của tổ chức, cá nhân; thông tin riêng, thông tin cá nhân và tài nguyên Internet.

3. Tạo, cài đặt, phát tán thư rác, tin nhắn rác, mã độc; thiết lập hệ thống thông tin lừa đảo, giả mạo.

4. Lợi dụng mạng để truyền bá thông tin, quan điểm, tài liệu, hình ảnh, âm thanh hoặc dạng thông tin khác nhằm thực hiện các hành vi gây lộ lột thông tin, ảnh hưởng đến an toàn, bí mật thông tin của cá nhân, cơ quan và ảnh hưởng đến an ninh quốc gia, trật tự, an toàn xã hội.

CHƯƠNG II

CÁC QUY ĐỊNH VỀ BẢO ĐẢM AN TOÀN, BẢO MẬT HỆ THỐNG CÔNG NGHỆ THÔNG TIN

Điều 6. Tổ chức quản lý vận hành chung

1.Thủ trưởng các đơn vị chịu trách nhiệm chỉ đạo công tác quản lý, phê chuẩn quy chế bảo đảm an toàn, ANTT đơn vị, phân công trách nhiệm từng bộ phận, cán

bộ, công chức, viên chức liên quan trong hoạt động khai thác, sử dụng hệ thống CNTT của cơ quan, đơn vị. Xây dựng và triển khai thực hiện quy chế an toàn, ANTT nội bộ cơ quan, đơn vị, trên cơ sở các chuẩn hiện hành của Nhà nước: TCVN ISO/IEC 27001: 2009 (ISO/IEC27001:2005), TCVN ISO/IEC27002:2011(IS0/IEC 27002:2005) để xây dựng quy chế an toàn, ANTT bảo đảm phù hợp với quy mô, điều kiện nhân lực, tài chính và mức độ chấp nhận rủi ro của đơn vị.

2. Lãnh đạo, từng phòng, ban và công chức, viên chức cam kết tuân thủ thực hiện các quy định bảo đảm an toàn, ANTT của đơn vị mình; đồng thời thực hiện các quy định bảo đảm an toàn, ANTT đối với các cá nhân, tổ chức khác khi giao dịch công việc.

3. Bảo đảm tính bảo mật, tính toàn vẹn, tính sẵn sàng, hiệu năng cao của hệ thống thông tin; khả năng chống chịu, khắc phục thảm họa do con người và thiên nhiên gây ra.

4. Phân loại, nhận biết, phân tích, đánh giá mức độ rủi ro an toàn thông tin, đồng thời xây dựng quy trình, thủ tục xử lý, khắc phục các rủi ro CNTT có thể xảy ra tại đơn vị. Xây dựng biểu mẫu thu thập, báo cáo các sự kiện rủi ro an toàn, ANTT; báo cáo tổng hợp định kỳ 6 tháng 1 lần về an toàn, ANTT của đơn vị cho cơ quan thẩm quyền cấp trên.

5. Bố trí nhân sự có năng lực chất lượng đảm nhận vị trí chuyên trách và tài chính phù hợp với quy mô cho công tác bảo đảm an toàn, ANTT của đơn vị.

Điều 7. Quản lý tài sản công nghệ thông tin

1. Cơ quan, đơn vị phải thống kê, kiểm kê tài sản (thiết bị phần cứng, phần mềm, tài liệu hệ thống, dữ liệu, phương tiện truyền thông lưu trữ, các dịch vụ hạ tầng CNTT và truyền thông; các tài sản hỗ trợ: thiết bị điều hòa, UPS), thông tin liên quan đến tài sản: Loại tài sản, số hiệu, vị trí, thông tin bản quyền, các mô tả khác cho việc thay thế, phục hồi, khắc phục sửa lỗi nhanh.

2. Phân loại tài sản CNTT theo mức độ giá trị tài chính, mức độ quan trọng, tầm ảnh hưởng đối với hệ thống để xây dựng nội quy, biện pháp kỹ thuật nghiệp vụ phù hợp bảo vệ dữ liệu, thông tin.

3. Phân công trách nhiệm cho từng công chức, viên chức, phòng, ban cụ thể trong việc sử dụng các tài sản CNTT, cam kết thực hiện các quy định bảo đảm an toàn, ANTT.

4. Phân loại thông tin: Tiến hành phân loại thông tin, dữ liệu theo mức độ nhạy cảm, giá trị của thông tin (từ tuyệt mật đến mật; từ riêng tư đến phổ biến) đối với đơn vị về tần xuất sử dụng, thời gian lưu trữ và giá trị pháp lý của nó, bảo đảm thông tin đó và tài sản gắn liền với các phương tiện xử lý thông tin một cách thích hợp cho việc phân loại.

Điều 8. Bảo đảm an toàn thông tin từ nguồn nhân lực

1. Phân công nhiệm vụ đối với từng cán bộ, công chức, viên chức ở từng vị trí công việc, bộ phận phải cam kết tuân thủ các quy định bảo đảm an toàn thông tin trong nội bộ; thường xuyên có kế hoạch đào tạo cho cán bộ, công chức, viên chức để nâng cao ý thức, trách nhiệm, kiến thức cơ bản và kỹ năng an toàn mạng, ANTT; đối với nhân viên mới được tuyển dụng cần phổ biến các quy định an toàn thông tin để khai thác và sử dụng hệ thống thông tin.

2. Phân công, bố trí công chức, viên chức chuyên trách về quản trị hệ thống thông tin có trình độ, năng lực phù hợp, đạo đức để vận hành quản lý hệ thống thông tin; cán bộ chuyên trách thường xuyên được huấn luyện, tập huấn nâng cao nghiệp vụ về an toàn, ANTT, đồng thời phải nghiên cứu, cập nhật các công nghệ an ninh hệ thống thông tin mới nhất để áp dụng tại đơn vị.

3. Trong quá trình làm việc, cơ quan, đơn vị phải lập kế hoạch phổ biến, cập nhật các quy định về an toàn, ANTT cho cán bộ, công chức, viên chức hàng năm để nhân viên hiểu rõ các quyền và trách nhiệm của họ đối với việc sử dụng an toàn tài sản CNTT. Kiểm tra việc thực hiện các nội quy, quy chế về an toàn, ANTT theo định kỳ.

4. Khi cán bộ, công chức, viên chức chuyển vị trí công tác hoặc nghỉ việc, cán bộ chuyên trách quản trị an ninh hệ thống cần phải tiến hành vô hiệu hóa, hủy bỏ quyền truy nhập hệ thống đối với nhân viên đó và bàn giao lại các tài liệu, hồ sơ, thông tin liên quan tới tài khoản bị hủy bỏ nhằm tránh tình trạng truy cập trái phép vào hệ thống, hoặc chuyển đổi tài khoản người dùng cho phù hợp với vị trí mới.

Điều 9. Bảo đảm an toàn vật lý và môi trường

1. Cơ quan, đơn vị phải thực hiện các biện pháp bảo vệ cần thiết để phòng tránh mất cắp, tai nạn hoặc phá hoại tại các vị trí lắp đặt các thiết bị xử lý và lưu trữ của hệ thống thông tin: Xây dựng tường rào, bố trí phòng lắp đặt thiết bị quan trọng, được khóa cẩn thận, có bảo vệ và kiểm soát khi vào phòng thiết bị của hệ thống, chỉ những người có quyền, nhiệm vụ mới được phép vào phòng.

2. Phân tích và đánh giá các mối đe dọa do thiên nhiên, con người như các thảm họa bão lũ, cháy nổ, lở đất, vật liệu độc hại, hoặc các mối đe dọa khác do thiên nhiên và con người gây ra rủi ro mất an toàn thông tin (xếp loại các mức độ đe dọa, điểm yếu kỹ thuật dễ bị tổn thương, các rủi ro từ mức cao đến thấp nhất); có kế hoạch phòng chống bão lũ, hệ thống chống sét, chống cháy nổ, bảo đảm áp dụng các quy chuẩn kỹ thuật về an toàn kỹ thuật nhiệt, độ ẩm, ánh sáng cho hệ thống máy chủ, các thiết bị hệ thống quan trọng khác.

3. Bảo đảm môi trường vật lý cho phòng máy chủ, các hệ thống hỗ trợ: máy điều hòa nhiệt độ, nguồn cấp điện, cáp quang truyền dẫn được an toàn và hoạt động ổn định, sẵn sàng.

4. Các thiết bị, phương tiện xử lý thông tin quan trọng, nhạy cảm của cơ quan, đơn vị phải được tách biệt khỏi nơi có đối tác thứ ba tham gia.

5. Chỉ cá nhân có quyền mới được truy nhập vào khu vực xử lý, lưu trữ thông tin quan trọng, nhạy cảm của cơ quan, đơn vị, với cơ chế kiểm tra xác thực thẻ có mã PIN.

6. Cần có kế hoạch kiểm tra, bảo dưỡng định kỳ các thiết bị hệ thống, duy trì phù hợp, đúng cách và an toàn với các yêu cầu thời gian và thông số kỹ thuật của nhà cung cấp.

Điều 10. Các biện pháp quản lý kỹ thuật cơ bản cho công tác an toàn, an ninh thông tin

1. Tổ chức mô hình mạng: Cài đặt, cấu hình, tổ chức hệ thống mạng theo mô hình Clients/Server, hạn chế sử dụng mô hình mạng ngang hàng. Khi thiết lập các dịch vụ trên môi trường mạng Internet, chỉ cung cấp những chức năng thiết yếu nhất

bảo đảm duy trì hoạt động của hệ thống thông tin; hạn chế sử dụng chức năng, cổng giao tiếp mạng, giao thức và các dịch vụ không cần thiết.

2. Quản lý hệ thống mạng không dây: Khi thiết lập mạng không dây để kết nối với mạng cục bộ thông qua các điểm truy nhập (Access Point -AP), cần thiết lập các tham số như: tên, SSID, mật khẩu, mã hóa dữ liệu. Khuyến cáo nên tắt chức năng WPS (Wi-Fi Protected Setup) và thông báo các thông tin liên quan đến AP để cơ quan sử dụng, định kỳ 3 tháng thay đổi mật khẩu nhằm tăng cường công tác bảo mật.

3. Chống mã độc, virus: Lựa chọn, triển khai các phần mềm bản quyền chống virus, thư rác trên các máy chủ, các thiết bị di động trong mạng và những hệ thống thông tin xung yếu như: Cổng thông tin điện tử, thư điện tử, một cửa điện tử,... để phát hiện, loại trừ những đoạn mã độc hại (Virus, trojan, worms,.) và hỗ trợ người sử dụng cài đặt các phần mềm này trên máy trạm. Các phần mềm này phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc khi sao chép, mở các tập tin. Thường xuyên cập nhật các phiên bản (Version) mới, các bản vá lỗi của các phần mềm chống virus để bảo đảm chương trình quét virus trên các máy chủ, máy trạm luôn được cập nhật mới nhất, thiết lập chế độ quét thường xuyên ít nhất là hằng tuần.

Nâng cao nhận thức của người dùng về cách sử dụng an toàn hệ thống thông tin, phòng chống mã độc, rủi ro do mã độc gây ra. Hạn chế truy cập wifi công cộng, miễn phí để thực hiện trao đổi công việc quản lý nhà nước. Khi phát hiện bất kỳ dấu hiệu nào liên quan đến việc nhiễm mã độc trên máy, người sử dụng cần tắt máy và báo trực tiếp đến bộ phận có trách nhiệm của đơn vị để xử lý.

4. Sao lưu dữ liệu dự phòng:

Ban hành và thực hiện quy trình sao lưu dữ liệu dự phòng và phục hồi cho các hệ thống thông tin và dữ liệu cần thiết.

Dữ liệu quan trọng của đơn vị phải được sao lưu, bao gồm: thông tin cấu hình, tập tin nhật ký của các thiết bị mạng, bảo mật, hệ điều hành; các phần mềm ứng dụng văn phòng, phần mềm chuyên ngành, cơ sở dữ liệu. Sau khi sao lưu mỗi máy được lưu vào các thiết bị lưu trữ như CD, ổ cứng ngoài,...và thực hiện việc đánh số, dán nhãn để tránh nhầm lẫn nhằm phục vụ cho công tác phục hồi dữ liệu một cách nhanh nhất.

Đối với máy chủ: Cài đặt các dịch vụ Mirror, Raid, Clustering, ...bảo đảm thiết lập cơ chế sao lưu và phục hồi hệ thống của máy chủ. Đối với các máy chủ cài đặt hệ điều hành Windows sử dụng chức năng System Restore để có thể dễ dàng khôi phục lại toàn bộ máy chủ hoặc các tập tin, thư mục được lựa chọn phục hồi.

5. Quản lý nhật ký trong quá trình vận hành các hệ thống thông tin:

Các đơn vị thực hiện việc ghi nhật ký (log) trên các thiết bị mạng máy tính, phần mềm ứng dụng, hệ điều hành, cơ sở dữ liệu nhằm đảm bảo các sự kiện quan trọng xảy ra trên hệ thống được ghi nhận và lưu giữ. Các nhật ký này phải được bảo vệ an toàn nhằm phục vụ công tác kiểm tra phân tích khi cần thiết. Đặc biệt, là hệ thống thông tin tại các bệnh viện.

Thường xuyên thực hiện việc theo dõi bản ghi nhật ký của hệ thống và các sự cố khác có liên quan để đánh giá, báo cáo các rủi ro và mức độ nghiêm trọng các rủi ro đó. Hạn chế việc tràn logfile gây ảnh hưởng đến hoạt động của hệ thống.

6. Quản lý điều khiển truy xuất:

- Ban hành chính sách, quy trình quản lý điều khiển truy xuất phù hợp với yêu cầu an toàn, ANTT của đơn vị, bao gồm các nội dung cơ bản sau đây: Đăng ký, cấp phát, gia hạn và thu hồi quyền của nhóm người dùng, người dùng; Nhất quán giữa chính sách kiểm soát truy cập và chính sách phân loại thông tin của các hệ thống thông tin khác nhau; Quản lý quyền truy cập trong môi trường mạng phân tán, mạng nội bộ và các kiểu kết nối mạng sẵn có; Thường xuyên kiểm tra, rà soát định kỳ, phân quyền người dùng gắn với trách nhiệm theo mức độ quan trọng của thông tin, tài sản CNTT; Quản lý cấp phát và vô hiệu, hủy bỏ mật khẩu người dùng trong trường hợp cần thiết; Đăng ký và đăng ký lại ID người dùng duy nhất gắn với trách nhiệm, vai trò của công chức, viên chức đó đối với tài sản CNTT được quyền truy cập; kiểm tra mức quyền truy cập hệ thống phù hợp với mục đích công việc của đơn vị; Yêu cầu các nhân viên hiểu được các quyền và cam kết thực hiện các điều kiện truy cập; Quản lý quyền truy cập gồm: Hệ điều hành, quản trị cơ sở dữ liệu, ứng dụng của đơn vị.

- Quản lý mật khẩu người dùng cần ban hành quy trình quản lý chính thức bảo đảm các yêu cầu sau: Quy định rõ trách nhiệm nhân viên đăng ký mật khẩu, ký cam kết giữ bí mật mật khẩu cá nhân và mật khẩu nhóm, sử dụng đúng quy định, không lưu trữ trên máy tính hay phương tiện không được bảo vệ; khi không sử dụng hệ thống cần phải thoát ra khỏi hệ thống; Mật khẩu tạm của thiết bị, sản phẩm CNTT của nhà sản xuất cung cấp hoặc các dịch vụ khác kết nối hệ thống CNTT của đơn vị phải được thay đổi khi đưa vào sử dụng chính thức; Quy định độ dài tối thiểu của mật khẩu trong hệ thống gồm ít nhất 06 ký tự (chữ, số và ký hiệu khác được chấp nhận của hệ thống), cần kiểm tra tính hợp lệ tự động mật khẩu khi đăng ký mật khẩu.

- Kiểm soát truy xuất mạng và dịch vụ mạng nhằm bảo vệ các truy xuất dịch vụ mạng của người không có thẩm quyền cả bên trong hệ thống của cơ quan, đơn vị và ngoài hệ thống. Đơn vị cần thiết lập cổng giao tiếp mạng nội bộ và mạng khác; các mạng công cộng có cơ chế xác thực hợp lý để bảo vệ truy xuất mạng không hợp lệ. Ban hành các quy định, thủ tục, các điều kiện cần thiết để truy cập mạng và dịch vụ mạng.

- Sử dụng chứng thực cho các kết nối từ xa bên ngoài mạng vào đơn vị đối với giải pháp mạng riêng ảo, khi kết nối dùng kỹ thuật mã hóa để bảo đảm an toàn, an ninh cho hệ thống.

- Ban hành chính sách kiểm soát truy cập hệ điều hành máy chủ bảo đảm chứng thực người dùng có thẩm quyền, phù hợp với một chính sách kiểm soát truy cập được xác định gồm: Mỗi người sử dụng hệ điều hành phải có một định danh duy nhất và được xác thực, nhận dạng, lưu dấu vết khi truy cập hệ điều hành, ghi nhận các truy cập thành công và thất bại; sử dụng phương tiện xác thực; quy định thời gian phiên làm việc đối với ứng dụng rủi ro cao, ngắt kết nối khi không làm việc.

- Kiểm soát chặt chẽ sử dụng các tiện ích hệ thống nhằm bảo đảm an toàn, an ninh hệ thống.

- Kiểm soát truy cập thông tin và ứng dụng: Phân quyền, nhóm quyền cho việc truy cập các thông tin, ứng dụng quan trọng theo chức năng, quyền hạn của nhân viên phù hợp với yêu cầu chính sách an ninh chung của đơn vị: Cung cấp các chức năng điều khiển người dùng: Ghi, xóa, đọc, thực thi lệnh; Các menu, chức năng

của ứng dụng; Bảo đảm thông tin quan trọng đầu ra được chuyển đến người có thẩm quyền.

7. Các biện pháp kỹ thuật bảo đảm an toàn cho Trang thông tin điện tử/ Cổng thông tin điện tử (gọi tắt là trang web):

- Xác định cấu trúc thiết kế trang web: Quản lý toàn bộ các phiên bản của mã nguồn, phối hợp với đơn vị thực hiện dịch vụ hosting tổ chức mô hình trang web hợp lý tránh khả năng tấn công leo thang đặc quyền. Yêu cầu đơn vị cung cấp dịch vụ hosting phải cài đặt các hệ thống phòng vệ như tường lửa (firewall), thiết bị phát hiện/phòng chống xâm nhập (IDS/IPS) ở mức ứng dụng web (WAF- Web Application Firewall).

- Vận hành ứng dụng web an toàn: Các trang web khi đưa vào sử dụng hoặc khi bổ sung thêm các chức năng, dịch vụ công mới cần liên hệ với các tổ chức an ninh mạng đánh giá kiểm định nhằm tránh được các lỗi bảo mật thường xảy ra trên ứng dụng web như: SQL Injection, Cross-Site Scripting (xss), Broken Authentication and Session Management, Insecure Direct Object References, Cross Site Request Forgery (CSRF), Security Misconfiguration, Failure to Restrict URL Access, Insecure Cryptographic Storage, Insufficient Transport Layer Protection, Unvalidated Redirects and Forwards,...

- Thiết lập và cấu hình cơ sở dữ liệu an toàn: Luôn cập nhật bản vá lỗi mới nhất cho hệ quản trị cơ sở dữ liệu; sử dụng công cụ để đánh giá, tìm kiếm lỗ hổng trên máy chủ cơ sở dữ liệu; Gỡ bỏ các cơ sở dữ liệu không sử dụng; Có các cơ chế sao lưu dữ liệu, tài liệu hóa quá trình thay đổi cấu trúc bằng cách xây dựng nhật ký CSDL với các nội dung như: nội dung thay đổi, lý do thay đổi, thời gian, vị trí thay đổi; Phối hợp với các nhà cung cấp dịch vụ hosting xây dựng phương án phục hồi trang web, trong đó chú ý mỗi tháng thực hiện việc backup toàn bộ nội dung trang web 1 lần bao gồm mã nguồn, cơ sở dữ liệu, dữ liệu phi cấu trúc,... để bảo đảm khi có sự cố có thể khắc phục lại ngay trong vòng 24 giờ.

Điều 11. Tiếp nhận, phát triển và bảo trì hệ thống thông tin

1. Khi đầu tư mới, nâng cấp hệ thống thông tin từ hệ thống hiện có đơn vị phải tiến hành phân tích các đặc điểm, tiêu chuẩn kỹ thuật yêu cầu an toàn, ANTT của hệ thống. Xử lý đúng các ứng dụng nhằm ngăn chặn các lỗi, sai, sử dụng trái phép hoặc sử dụng thông tin sai trong ứng dụng; thực hiện các cơ chế kiểm soát dữ liệu đầu vào hợp lệ, quá trình xử lý bên trong hệ thống và kết xuất thông tin phải bảo đảm chính xác, thích hợp với hoạt động của cơ quan, đơn vị.

2. Giao trách nhiệm cho các công chức, viên chức liên quan trong quá trình xử lý nhập thông tin vào hệ thống ứng dụng; tạo nhật ký ghi quá trình nhập dữ liệu vào hệ thống.

3. Kiểm tra xác nhận xử lý dữ liệu bên trong ứng dụng nhằm phát hiện ngăn chặn các chế biến dữ liệu trái phép, hành vi cố ý khác làm mất an toàn thông tin (các yếu tố cần xem xét như sử dụng chức năng thêm, xóa, sửa dữ liệu); sử dụng các chương trình phục hồi thích hợp nhằm phục hồi các xử lý thất bại để bảo đảm chính xác, toàn vẹn của xử lý dữ liệu.

4. Kiểm tra tính xác thực, tính toàn vẹn hoặc bất kỳ tính năng bảo mật dữ liệu đối với phần mềm khác tải về hoặc tải lên, giữa các máy tính trung tâm và máy từ

xa; kiểm tra tính hợp lệ của dữ liệu xuất ra từ các ứng dụng, bảo đảm quá trình xử lý thông tin của các ứng dụng là chính xác và hợp lệ.

5. Quản lý mã hóa và khóa phải được áp dụng đối với thông tin tối quan trọng của đơn vị (thông tin lưu trữ và truyền tải qua mạng hay các phương tiện khác) nhằm bảo đảm tính bảo mật, xác thực và ràng buộc toàn vẹn của thông tin bằng các giải thuật, phương pháp được quy định chuẩn do quốc tế và quốc gia công nhận gồm:

- Giải thuật RSA (Rivest-Shamir-Adleman);

- Giải thuật băm cho chữ ký số SHA-2 (Secure Hash Algorithm);

- Mã hóa giải thuật 3DES (Triple Data Encryption Standard);

- Giải pháp xác thực người sử dụng SAML v2.0 (Security Assertion Markup Language);

- An toàn trao đổi bản tin XML (XML Encryption Syntax and Processing);

- AES: Advanced Encryption Standard;

- Các giải thuật khác theo chuẩn quy định của Bộ Thông tin và Truyền thông.

6. Bảo đảm an toàn, bảo mật tệp hệ thống và các mã nguồn của phần mềm dự án CNTT: Ban hành quy định, quy trình cài đặt, nâng cấp các phần mềm ứng dụng của cơ quan, đơn vị, hệ điều hành máy chủ, các thư viện của chương trình ứng dụng. Công chức, viên chức chuyên trách về quản trị hệ thống cần được huấn luyện, cập nhật kiến thức, tiêu chuẩn, chức năng của phần mềm được nâng cấp phù hợp với hệ thống hiện tại; lưu trữ an toàn tài liệu tệp cấu hình hệ thống hiện tại, các phiên bản phần mềm ứng dụng trước được lưu trữ như biện pháp dự phòng, có kế hoạch phục hồi lại hoàn toàn trước khi các thay đổi được thực hiện.

7. Khi thay đổi hệ điều hành phiên bản mới hơn cần xem xét tính tương thích với các ứng dụng hiện có, bảo đảm hệ thống hoạt động ổn định, an toàn; kiểm soát chặt chẽ việc nâng cấp, mở rộng các gói phần mềm ứng dụng trong hệ thống (các mô đun chương trình ứng dụng), hạn chế việc thay đổi các gói phần mềm đang sử dụng.

8. Đối với các đối tác cung cấp các chương trình ứng dụng, phần mềm nghiệp vụ cần quy định an toàn, ANTT, chỉ cho phép truy cập vật lý và logic hệ thống khi thực sự cần thiết và có sự chấp thuận của người có thẩm quyền, các hoạt động của đối tác phải được giám sát, quản lý chặt chẽ.

9. Các thông tin (tài khoản cá nhân, dữ liệu quan trọng) không được dùng cho mục đích thử nghiệm chương trình (như ứng dụng cơ sở dữ liệu).

10. Bảo đảm an toàn, ANTT trong quy trình hỗ trợ và phát triển: Phải có quy định kiểm soát khi có sự thay đổi hệ thống, cần phân tích đánh giá tác động của thay đổi phần mềm hệ thống đối với đơn vị, sự thay đổi phải được chấp thuận của người có thẩm quyền.

11. Quản lý lỗ hổng kỹ thuật dễ bị tổn thương cần thực hiện thường xuyên, xem xét phân tích đánh giá các tổn thương kỹ thuật trong hệ thống thông tin nhằm hạn chế rủi ro an toàn thông tin; định nghĩa, thiết lập vai trò và trách nhiệm quản lý các điểm yếu về kỹ thuật bao gồm việc giám sát điểm yếu kỹ thuật, đánh giá các rủi ro tiềm ẩn, theo dõi tài sản và bất cứ trách nhiệm điều phối yêu cầu cần thiết khác. Định kỳ đánh giá, lập báo cáo về các điểm yếu kỹ thuật của các hệ thống CNTT

đang sử dụng. Xây dựng giải pháp, hệ thống giám sát, phát hiện, ngăn chặn việc tấn công các điểm yếu kỹ thuật nhằm hạn chế rủi ro ANTT.

Điều 12. Quản lý truyền thông và hoạt động

1. Tài liệu quy trình thủ tục hoạt động hệ thống và các phương tiện xử lý thông tin và truyền thông được chuẩn bị, duy trì, cập nhật và phân phối đến tất cả công chức, viên chức có trách nhiệm đối với tài sản CNTT liên quan, gồm các hoạt động: Quy trình khởi động, tắt máy tính; duy trì các phương tiện lưu trữ (sao chép dự phòng, phục hồi dữ liệu); bảo trì thiết bị phần cứng; quản lý, khắc phục sự cố, lỗi xảy ra trong quá trình vận hành thiết bị CNTT; quản lý thông tin nhật ký hệ thống, các quy trình xử lý Email an toàn.

2. Các quy trình, tài liệu hướng dẫn vận hành phải được phê duyệt của người quản lý có thẩm quyền, được cập nhật cho phù hợp với điều kiện môi trường, công nghệ thay thế mới.

3. Kiểm soát sự thay đổi các thiết bị hệ thống, phương tiện CNTT và truyền thông (phần cứng, phần mềm, công cụ hỗ trợ chuyên môn) gồm các hoạt động: Nhận dạng và thu thập các thay đổi tiêu chuẩn kỹ thuật của thiết bị, công tác đánh giá tác động tiềm năng do thay đổi đối với hoạt động chung của hệ thống, phổ biến sự thay đổi đến tất cả các cá nhân có liên quan sử dụng hệ thống, xem xét khả năng nâng cấp các phiên bản của ứng dụng, hệ điều hành ảnh hưởng đến hệ thống, ghi chép lại các thay đổi; lập kế hoạch thực hiện và kiểm tra, thử nghiệm sự thay đổi trước khi áp dụng chính thức.

4. Không phát triển, kiểm thử, cài đặt các ứng dụng thử nghiệm trên hệ thống vận hành chính thức để giảm thiểu rủi ro về an toàn thông tin.

5. Bảo đảm quản lý dịch vụ do các đối tác bên ngoài cơ quan cung cấp: Khi đối tác thứ ba cung cấp dịch vụ, cần thỏa thuận bằng các văn bản hợp đồng bảo đảm về ANTT (gia công chuyển đổi, phương tiện xử lý thông tin, hay bất cứ hoạt động liên quan đến tài sản CNTT của cơ quan, đơn vị); giám sát và xem xét lại việc thực hiện cấp độ các dịch vụ để tuân thủ các thỏa thuận hợp đồng, trách nhiệm quản lý liên quan đến đối tác phải gắn với cá nhân được chỉ định và nhóm quản lý.

6. Quản lý các thay đổi đối với các dịch vụ của bên thứ ba cung cấp bao gồm: Nâng cấp phiên bản mới; sử dụng các kỹ thuật mới, các công cụ và môi trường phát triển mới. Đánh giá đầy đủ tác động của việc thay đổi, bảo đảm an toàn khi được đưa vào sử dụng; cập nhật các quy định, tiêu chuẩn an toàn, ANTT mới cho phù hợp với các thay đổi sản phẩm và dịch vụ mới do bên thứ ba cung cấp.

7. Lập kế hoạch hệ thống và chấp nhận hệ thống thông tin (gồm xây dựng hệ thống thông tin mới, nâng cấp, phiên bản ứng dụng mới) cần đáp ứng các yêu cầu cho tương lai về dung lượng, hiệu năng, tính sẵn sàng, thời gian phục hồi khi có sự cố của hệ thống, khả năng mở rộng hệ thống. Thiết lập các yêu cầu hoạt động hệ thống mới cần tài liệu hướng dẫn, chuyển giao công nghệ cho người dùng và kiểm thử trước khi chấp nhận đưa vào sử dụng chính thức.

8. Kiểm soát chống các mã độc bằng các phương tiện giám sát, ngăn chặn; ban hành các quy định chính thức cấm sử dụng các phần mềm trái phép trong hệ thống khi chưa có sự chấp thuận của người thẩm quyền.

9. Chính sách ngăn chặn các virus, trojan, worms lây lan qua mạng Internet, qua tệp dữ liệu sao chép, hay bất cứ phương tiện khác: cài đặt, nâng cấp thường

xuyên các phần mềm diệt vi rút; thiết lập các hệ thống an ninh phát hiện, chống xâm nhập (IDS/IPS); kiểm tra, diệt vi rút, mã độc cho toàn bộ hệ thống CNTT của cơ quan, đơn vị hàng ngày và phương tiện mang tin nhận từ bên ngoài trước khi sử dụng. Đối với cổng/trang tin điện tử cần vận hành, kiểm tra ứng dụng Web an toàn, tổ chức tường lửa (firewall) cứng hoặc bằng phần mềm, sử dụng các giao thức SSL để mã hóa kết nối an toàn, đối phó tấn công từ chối dịch vụ (DDoS) cần vô hiệu hóa các hoạt động botnet.

10. Chuẩn bị các kế hoạch duy trì hoạt động liên tục của đơn vị từ các cuộc tấn công, kế hoạch phục hồi và sao chép dữ liệu, phần mềm dự phòng.

11. Nâng cao nhận thức người dung chỉ truy cập các trang web đáng tin cậy, không tải các tài liệu đính kèm không rõ nguồn từ các trang web lạ.

12. Lập danh sách các dữ liệu, phần mềm cần được sao lưu, có phân loại theo thời gian lưu trữ, thời gian sao lưu, phương pháp sao lưu và thời gian kiểm tra phục hồi hệ thống từ dữ liệu sao lưu.

13. Xây dựng và thực hiện quy trình sao lưu dự phòng dữ liệu, phần mềm, phương pháp phục hồi dữ liệu và phần mềm khi có sự cố hệ thống. Dữ liệu, thiết bị sao lưu dự phòng cần lưu giữ ở nơi an toàn, bảo đảm an ninh.

14. Quản lý an toàn, an ninh mạng cần thực hiện các công tác ngăn chặn các kết nối mạng không có thẩm quyền, ban hành trách nhiệm và các thủ tục truy nhập mạng từ xa (mạng riêng ảo) cho cá nhân được phép; có các cơ chế đặc biệt nhằm bảo vệ dữ liệu, thông tin nhạy cảm của cơ quan, đơn vị truyền tải qua mạng công cộng hoặc kết nối không dây phải được bảo vệ để bảo toàn tính toàn vẹn và bí mật của thông tin; lưu trữ đầy đủ sơ đồ logic và bản vẽ hệ thống mạng.

15. Áp dụng các công nghệ an toàn dịch vụ mạng như mã hóa thông tin, cơ chế xác thực, và các kiểm soát kết nối mạng khác bảo đảm thiết lập, cấu hình đúng các tham số, tính năng yêu cầu an toàn của thiết bị mạng.

16. Xây dựng và ban hành quy định, thủ tục trao đổi thông tin giữa cơ quan, đơn vị với các tổ chức, cá nhân bên ngoài phải bảo đảm an toàn, ANTT như phát hiện tệp đính kèm có mã độc, cơ chế bảo mật truyền thông không dây, trao đổi tài liệu điện tử trên mạng. Xác định trách nhiệm và nghĩa vụ pháp lý đối với các thành phần tham gia.

17. Giao dịch trực tuyến phải được truyền đầy đủ, đúng địa chỉ, tránh bị sửa đổi, tiết lộ hoặc nhân bản một cách trái phép; sử dụng các cơ chế xác thực mạnh, chữ ký số khi tham gia giao dịch, sử dụng các nghi thức truyền thông an toàn.

18. Công chức, viên chức chuyên trách quản trị hệ thống phải duy trì thường xuyên hoạt động giám sát, ghi nhật ký hệ thống CNTT và người dùng; các sự kiện an ninh hệ thống, lỗi truy nhập trùng lắp phải được ghi lại nhằm trợ giúp cho việc điều tra giám sát, khắc phục sự cố về sau. Phải kiểm toán nhật ký hệ thống thường xuyên: Tài khoản người dùng, ngày, giờ, và chi tiết của sự kiện quan trọng như: Đăng nhập và xuất; ghi dấu vết các cố gắng truy xuất (thành công và từ chối) của hệ thống, cơ sở dữ liệu, thay đổi cấu hình hệ thống, các nghi thức và địa chỉ mạng truy nhập. Phương tiện lưu trữ nhật ký hệ thống và thông tin nhật ký phải được bảo vệ an toàn, bảo mật, không được sửa đổi, xóa bỏ.

19. Thiết lập đồng hồ của tất cả các hệ thống xử lý thông tin có liên quan trong một tổ chức, lĩnh vực an ninh nên được đồng bộ với một nguồn thời gian chính xác, đồng bộ.

Điều 13. Quản lý sự cố an ninh thông tin

1. Xây dựng các mẫu báo cáo sự kiện ANTT, thủ tục báo cáo về sự kiện an toàn thông tin, xác định rõ cá nhân có trách nhiệm tiếp nhận báo cáo sự cố ANTT bảo đảm luôn luôn sẵn sàng và đáp ứng khắc phục sự cố kịp thời.

2. Tất cả bộ phận, công chức, viên chức liên quan phải nhận thức trách nhiệm về báo cáo sự kiện ANTT càng sớm càng tốt, phải có thủ tục phản hồi kết quả báo cáo sự kiện ANTT sau khi vấn đề được khắc phục và giải quyết sự cố hoàn tất; xác định rõ trách nhiệm về báo cáo ANTT đối với cá nhân, bộ phận cụ thể.

3. Quy định thủ tục xử lý kỷ luật chính thức đối với nhân viên, nhà thầu hoặc người sử dụng của bên thứ ba có hành vi vi phạm ANTT.

4. Các sự kiện sự cố ANTT dưới đây cần được xem xét báo cáo:

- Hệ thống trục trặc nhiều lần hoặc quá tải.

- Mất thiết bị, phương tiện CNTT.

- Không tuân thủ chính sách ANTT hoặc các chỉ dẫn bắt buộc của đơn vị hoặc hành vi vi phạm an ninh vật lý.

- Không kiểm soát được hệ thống thông tin khi thay đổi.

- Các trục trặc của phần mềm hay phần cứng không khắc phục được.

- Những truy cập trái phép, hành vi vi phạm bảo mật và tính toàn vẹn.

- Phát hiện mã độc mới, tấn công từ chối dịch vụ.

- Lỗi kết quả đầu ra dữ liệu, thông tin sai, không chính xác.

5. Tất cả công chức, viên chức, đối tác thứ ba, nhà thầu tham gia vào hệ thống thông tin của cơ quan, đơn vị cần lưu ý, báo cáo bất kỳ quan sát nghi ngờ các điểm yếu của hệ thống thông tin và dịch vụ nhằm ngăn chặn các sự cố ANTT.

6. Ban hành thủ tục, quy định trách nhiệm đối với cá nhân, bộ phận liên quan trong cơ quan, đơn vị để giải quyết, khắc phục sự cố ANTT; các bước hành động khẩn cấp khắc phục sự cố cần được ghi vào tài liệu lưu trữ chi tiết. Trong điều kiện năng lực hiện có của đơn vị phải dùng mọi biện pháp cần thiết khắc phục sự cố càng sớm càng tốt nhằm giảm thiểu rủi ro an toàn thông tin.

7. Thu thập, ghi chép và bảo toàn các chứng cứ được ghi nhận về sự cố ANTT phục vụ cho công tác kiểm tra, xử lý, khắc phục sự cố an toàn thông tin; đơn vị có trách nhiệm cung cấp các bằng chứng liên quan đến sự cố ANTT cho cơ quan thẩm quyền theo quy định của pháp luật.

Điều 14. Quản lý bảo đảm hoạt động liên tục hệ thống thông tin

1. Cơ quan, đơn vị phải xây dựng kế hoạch và thực hiện quy trình bảo đảm duy trì hoạt động liên tục các hệ thống CNTT trọng yếu của cơ quan, đơn vị nhằm giảm thiểu những tác động làm gián đoạn công việc, hoạt động của cơ quan, đơn vị. Nhận dạng và đánh các giá mức độ rủi ro ANTT trong quy trình xử lý công việc của cơ quan, đơn vị (từ mức độ nhẹ đến nghiêm trọng) có thể xảy ra để có biện pháp ứng phó, khắc phục kịp thời bảo đảm hoạt động liên tục của hệ thống.

2. Thường xuyên tiến hành định kỳ 6 tháng 1 lần thực hiện kiểm tra, đánh giá, cập nhật quy trình bảo đảm duy trì hoạt động liên tục của hệ thống thông tin của cơ quan, đơn vị.

3. Quy định trách nhiệm, các thỏa thuận bảo đảm hoạt động liên tục của hệ thống thông tin đối với các công chức, nhân viên chuyên trách quản trị hệ thống. Huấn luyện nâng cao nhận thức, kỹ năng cho công chức, nhân viên về các quy trình khắc phục sự cố ANTT bảo đảm hoạt động liên tục của hệ thống thông tin.

4. Các thủ tục tạm thời hoạt động chờ khắc phục sự cố, hoạt động ứng cứu khẩn cấp sau khi xảy ra sự cố ANTT cần được mô tả đầy đủ, chi tiết nhằm khắc phục sự cố bảo đảm hoạt động liên tục hệ thống thông tin của cơ quan, đơn vị.

CHƯƠNG III

TỔ CHỨC THỰC HIỆN

Điều 15. Trách nhiệm của cơ quan Sở Y tế và các đơn vị trực thuộc

1. Các đơn vị chịu trách nhiệm toàn diện trước Giám đốc Sở trong công tác bảo đảm an toàn, an ninh cho hệ thống thông tin tại đơn vị, đồng thời thực hiện nghiêm túc các quy định tại Quy chế này.

2. Khi có sự cố hoặc nguy cơ mất an toàn, ANTT, kịp thời áp dụng mọi biện pháp để khắc phục và hạn chế thiệt hại; tiến hành lập biên bản, báo cáo bằng văn bản về Văn phòng Sở.

3. Báo cáo tình hình và kết quả thực hiện công tác bảo đảm an toàn, ANTT tại đơn vị và gửi về Văn phòng Sở 6 tháng 1 lần.

Điều 16. Trách nhiệm của cán bộ, công chức, viên chức tại cơ quan Sở Y tế và các đơn vị trực thuộc

1. Trách nhiệm của cán bộ chuyên trách CNTT :

- Chịu trách nhiệm triển khai các biện pháp quản lý vận hành, quản lý kỹ thuật và tham mưu xây dựng các quy định bảo đảm an toàn, ANTT cho hệ thống thông tin tại đơn vị mình theo các quy định của Quy chế này; thường xuyên cập nhật, nâng cấp các thủ tục, quy trình hoạt động an toàn, an ninh hệ thống cho đơn vị bảo đảm an toàn hệ thống thông tin.

- Phối hợp với các cá nhân, đơn vị liên quan trong việc kiểm tra, phát hiện và khắc phục sự cố mất an toàn, ANTT.

2. Trách nhiệm của cán bộ, công chức, viên chức:

Nghiêm chỉnh thi hành các quy chế nội bộ, quy trình về an toàn, ANTT của đơn vị cũng như các quy định khác của pháp luật; nâng cao ý thức cảnh giác, trách nhiệm bảo đảm an toàn, ANTT tại đơn vị.

Điều 17. Khen thưởng và xử lý vi phạm

1. Khen thưởng và xử lý vi phạm theo Quy định này được đưa vào tiêu chuẩn đánh giá mức độ hoàn thành nhiệm vụ và xét thi đua, khen thưởng hằng năm của của cơ quan Sở Y tế và các đơn vị trực thuộc Sở.

2. Tổ chức, cá nhân vi vi phạm quy chế này tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật theo trách nhiệm, xử phạt hành chính hoặc bị truy cứu

trách nhiệm hình sự. Nếu gây thiệt hại phải bồi thường theo quy định của pháp luật hiện hành.

Điều 18. Điều khoản thi hành

1. Chánh Văn phòng, Trưởng các phòng chức năng cơ quan Sở Y tế, Thủ trưởng các đơn vị trực thuộc và cán bộ, công chức, viên chức cơ quan Sở Y tế và các đơn vị trực thuộc chịu trách nhiệm thực hiện theo đúng quy chế này.

2. Trong quá trình triển khai thực hiện, nếu có vấn đề vướng mắc phát sinh, các đơn vị báo cáo về Sở Y tế để xem xét, điều chỉnh, bổ sung cho phù hợp./.

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ Y TẾ

Nguyễn Tấn Đức

UBND TỈNH QUẢNG NGÃI
SỞ Y TẾ

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

Số: 3887 /QĐ-SYT

Quảng Ngãi, ngày 11 tháng 11 năm 2015

QUYẾT ĐỊNH
Ban hành Quy chế bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin trong toàn ngành Y tế tỉnh Quảng Ngãi

Căn cứ Luật Giao dịch điện tử ngày 29 tháng 11 năm 2005;

Căn cứ Luật Công nghệ thông tin ngày 29 tháng 6 năm 2006;

Căn cứ Nghị định số 63/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ quy định xử phạt vi phạm hành chính trong lĩnh vực công nghệ thông tin;

Căn cứ 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;

Căn cứ Nghị định số 72/2013/NĐ-CP ngày 15 tháng 7 năm 2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng;

Căn cứ Chỉ thị số 897/CT-TTg ngày 10 tháng 6 năm 2011 của Thủ tướng Chính phủ về việc triển khai các hoạt động đảm bảo an toàn thông tin số;

Căn cứ Thông tư số 22/2013/TT-BTTTT ngày 23 tháng 12 năm 2013 của Bộ Thông tin và Truyền thông về công bố danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước;

Căn cứ Thông tư số 25/2014/TT-BTTTT ngày 30 tháng 12 năm 2014 của Bộ Thông tin và Truyền thông về quy định về triển khai các hệ thống thông tin có quy mô và phạm vi từ Trung ương đến địa phương;

Căn cứ Quyết định số 44/2012/QĐ-UBND ngày 06/12/2012 của UBND tỉnh Quảng Ngãi về Ban hành Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan, đơn vị quản lý nhà nước tỉnh Quảng Ngãi;

Căn cứ Quyết định 213/QĐ-UBND ngày 06/08/2008 của UBND tỉnh Quảng Ngãi về ban hành Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức bộ máy của Sở Y tế tỉnh Quảng Ngãi;

Theo đề nghị của Chánh Văn phòng Sở Y tế,

QUYẾT ĐỊNH:

Điều 1: Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin trong toàn ngành Y tế tỉnh Quảng Ngãi.

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