ỦY BAN NHÂN DÂN TỈNH QUẢNG NGÃI	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 44/2012/QĐ-UBND	*Quảng Ngãi, ngày 06 tháng 12 năm 2012*

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm 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

ỦY BAN NHÂN DÂN TỈNH QUẢNG NGÃI

Căn cứ Luật Tổ chức HĐND và UBND ngày 26/11/2003;

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

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

Căn cứ Nghị định số 63/2007/NĐ-CP ngày 10/4/2007 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 10/4/2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

Căn cứ Chỉ thị số 03/2007/CT-BBCVT ngày 23/02/2007 của Bộ Bưu chính, Viễn thông về việc tăng cường bảo đảm an ninh thông tin trên mạng Internet;

Căn cứ Thông tư số 01/2011/TT-BTTTT ngày 04/01/2011 của Bộ Thông tin và Truyền thông công bố Danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước;

Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Tờ trình số 345/TTr-STTTT ngày 29/6/2012 và Báo cáo thẩm tra số 96/BC-STP ngày 13/6/2012 của Sở Tư pháp về việc ban hành Quy chế bảo đảm 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,

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 của các cơ quan, đơn vị quản lý nhà nước tỉnh Quảng Ngãi.

Điều 2. Quyết định này có hiệu lực thi hành sau 10 ngày, kể từ ngày ký.

Điều 3. Chánh Văn phòng UBND tỉnh; Thủ trưởng các sở, ban ngành tỉnh; Chủ tịch UBND các huyện, thành phố chịu trách nhiệm thi hành Quyết định này./.

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Lê Quang Thích

ỦY BAN NHÂN DÂN TỈNH QUẢNG NGÃI	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc

QUY CHẾ

Bảo đảm 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

(Ban hành kèm theo Quyết định số: 44/2012/QĐ-UBND ngày 06 tháng 12 năm 2012 của Ủy ban nhân dân tỉnh Quảng Ngãi)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Đối tượng áp dụng

1. Quy chế này áp dụng đối với các cơ quan, đơn vị quản lý nhà nước trên địa bàn tỉnh, bao gồm: các sở, ban, ngành trực thuộc UBND tỉnh, UBND các huyện, thành phố Quảng Ngãi *(sau đây gọi tắt là cơ quan, đơn vị)*.

2. Công chức, viên chức đang làm việc tại các đơn vị sự nghiệp trực thuộc các cơ quan, đơn vị quản lý nhà nước quy định tại Khoản 1 Điều này, các cá nhân, tổ chức có liên quan khi tham gia vận hành, khai thác, sử dụng hệ thống công nghệ thông tin (CNTT) tại các cơ quan, đơn vị quản lý nhà nước quy định tại Khoản 1, Điều này.

Điều 2. Phạm vi điều chỉnh

Quy chế này quy định các nội dung của công tác bảo đảm an toàn, an ninh thông tin (ANTT) trong hoạt động ứng dụng CNTT của các cơ quan, đơn vị quản lý nhà nước thuộc tỉnh Quảng Ngãi, bao gồm: Xây dựng các quy định về bảo đảm an toàn, an ninh hệ thống thông tin; trách nhiệm của các cơ quan, cá nhân liên quan thực hiện bảo đảm an toàn, ANTT trong cơ quan, đơn vị.

Điều 3. Mục đích bảo đảm 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 cơ quan, đơn vị quản lý nhà nước 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 cơ quan, đơn vị quản lý nhà nước phải bảo đảm tính bảo mật, an toàn, ANTT, hợp lý và hiệu quả.

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 cơ quan, 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 cơ quan, 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 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.

Chương II

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

Điều 5. Tổ chức quản lý vận hành chung

1. Thủ trưởng cơ quan, đơn vị chịu trách nhiệm chỉ đạo công tác quản lý, phê chuẩn quy chế bảo đảm an toàn, ANTT của cơ quan, 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/IEC 27001:2005), TCVN ISO/IEC 27002:2011(ISO/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 cơ quan, 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 cơ quan, 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 trong cơ quan, 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 cơ quan, 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 cơ quan, đơn vị.

Điều 6. 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 cơ quan, 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 7. Bảo đảm an toàn thông tin từ nguồn nhân lực

1. Cơ quan, đơn vị cần 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 cơ quan, 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 8. 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 9. Quản lý điều khiển truy xuất

1. Ban hành chính sách, quy trình quản lý điều khiển truy xuất phù hợp với yêu cầu an toàn, ANTT của cơ quan, đơn vị, bao gồm các nội dung cơ bản sau đây:

a) Đăng ký, cấp phát, gia hạn và thu hồi quyền của nhóm người dùng, người dùng.

b) Nhất quán giữa chính sách kiểm soát truy cập và chính sách phân loại thông tin của các hệ thống thông tin khác nhau.

c) Quản lý quyền truy cập trong môi trường mạng phân tán, mạng nội bộ và các kiểu kết nối mạng sẵn có.

d) 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.

đ) Quản lý cấp phát và vô hiệu, hủy bỏ mật khẩu người dùng trong trường hợp cần thiết.

e) 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.

g) Yêu cầu các nhân viên hiểu được các quyền và cam kết thực hiện các điều kiện truy cập.

h) Quản lý quyền truy cập gồm: Hệ điều hành, quản trị cơ sở dữ liệu, ứng dụng của đơn vị.

2. Quản lý mật khẩu người dùng cần ban hành quy trình quản lý chính thức bảo đảm các yêu cầu sau:

a) 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.

b) 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 cơ quan, đơn vị phải được thay đổi khi đưa vào sử dụng chính thức.

c) 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.

3. 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. Cơ quan, 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.

4. Sử dụng chứng thực cho các kết nối từ xa bên ngoài mạng vào cơ quan, 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.

5. 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.

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

7. 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:

a) Cung cấp các chức năng điều khiển người dùng: Ghi, xóa, đọc, thực thi lệnh;

b) Các menu, chức năng của ứng dụng;

c) Bảo đảm thông tin quan trọng đầu ra được chuyển đến người có thẩm quyền.

Điều 10. 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, cơ quan, đơn vị phải tiến hành phân tích các đặc điểm, tiêu chuẩn kỹ thuật yêu cầu an toàn, ANTT của hệ thống, thực hiện đồng thời với quy trình nghiệp vụ của cơ quan, đơn vị nhằm kiểm soát an toàn, ANTT; kiểm soát ANTT được thiết kế, mô tả rõ ràng, đầy đủ ngay từ lúc khởi động thiết kế một dự án CNTT, yêu cầu các bên cung cấp, thi công dự án

bảo đảm đúng yêu cầu về an toàn thông tin theo các tiêu chuẩn kỹ thuật của Bộ Thông tin và Truyền thông đã ban hành.

2. 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. Để bảo đảm dữ liệu hợp lệ và ngăn chặn các sai sót do nhập vào hệ thống, cần có kiểm tra tự động từ ứng dụng (như vùng hợp lệ dữ liệu, kiểu dữ liệu, dữ liệu không đầy đủ), cần xem xét lại định kỳ các nội dung thông tin quan trọng và xác nhận tính tin cậy và hợp lệ của dữ liệu, bảo đảm tính ràng buộc toàn vẹn dữ liệu khi thiết kế cơ sở dữ liệu.

3. 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.

4. 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.

5. 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.

6. Quản lý mã hóa và khóa phải được áp dụng đối với thông tin tối quan trọng của cơ quan, 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:

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

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

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

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

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

e) AES: Advanced Encryption Standard;

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

7. 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.

8. 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.

9. 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.

10. 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).

11. 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 cơ quan, đơn vị, sự thay đổi phải được chấp thuận của người có thẩm quyền.

12. 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 11. 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 E-mail 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 dùng 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 12. 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:

a) Hệ thống trục trặc nhiều lần hoặc quá tải;

b) Mất thiết bị, phương tiện CNTT;

c) Không tuân thủ chính sách ANTT hoặc các chỉ dẫn bắt buộc của cơ quan, đơn vị hoặc hành vi vi phạm an ninh vật lý;

d) Không kiểm soát được hệ thống thông tin khi thay đổi;

đ) Các trục trặc của phần mềm hay phần cứng không khắc phục được;

e) Những truy cập trái phép, hành vi vi phạm bảo mật và tính toàn vẹn;

g) Phát hiện mã độc mới, tấn công từ chối dịch vụ;

h) 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 cơ quan, 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; cơ quan, 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 13. 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

TRÁCH NHIỆM ĐẢM BẢO AN TOÀN, BẢO MẬT THÔNG TIN

Điều 14. Trách nhiệm của các cơ quan, đơn vị quản lý nhà nước

1. Thủ trưởng các cơ quan, đơn vị chịu trách nhiệm toàn diện trước Ủy ban nhân dân tỉnh trong công tác bảo đảm an toàn, an ninh cho hệ thống thông tin của cơ quan, đơn vị đó, 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 cho cơ quan cấp trên quản lý trực tiếp và Sở Thông tin và Truyền thông. Trường hợp có sự cố nghiêm trọng vượt quá khả năng khắc phục của đơn vị, phải báo cáo ngay cho cơ quan cấp trên quản lý trực tiếp và Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ.

3. Phối hợp với đoàn kiểm tra do Sở Thông tin và Truyền thông chủ trì để triển khai công tác kiểm tra, khắc phục sự cố an toàn, an ninh thông tin trong hệ thống thông tin của cơ quan, đơn vị, đồng thời cung cấp đầy đủ các thông tin về an toàn, an ninh thông tin khi đoàn kiểm tra yêu cầu.

4. Báo cáo tình hình và kết quả thực hiện công tác bảo đảm an toàn, ANTT tại cơ quan, đơn vị và gửi về Sở Thông tin và Truyền thông định kỳ 6 tháng 1 lần.

Điều 15. Trách nhiệm của Sở Thông tin và Truyền thông

1. Tham mưu Ủy ban nhân dân tỉnh về công tác bảo đảm an toàn, ANTT trên địa bàn tỉnh và chịu trách nhiệm trước Ủy ban nhân dân tỉnh trong việc bảo đảm an toàn, ANTT cho các hệ thống thông tin cấp tỉnh.

2. Xây dựng và triển khai các chương trình đào tạo, hội nghị tuyên truyền bảo

đảm an toàn, ANTT trong công tác quản lý hành chính nhà nước trên địa bàn tỉnh.

3. Hướng dẫn các cơ quan, đơn vị thực hiện các báo cáo về sự cố mất an toàn, ANTT và kết quả thực hiện công tác bảo đảm an toàn, ANTT tại các cơ quan, đơn vị.

4. Chủ trì, phối hợp với Văn phòng Ủy ban nhân dân tỉnh, Công an tỉnh và các đơn vị có liên quan tiến hành kiểm tra công tác bảo đảm an toàn, an ninh thông tin định kỳ hàng năm đối với các cơ quan, đơn vị quản lý nhà nước thuộc tỉnh.

5. Tùy theo mức độ sự cố, phối hợp Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) và các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố mất an toàn, ANTT.

Điều 16. Trách nhiệm của Công an tỉnh

1. Phối hợp với Sở Thông tin và Truyền thông kiểm tra công tác bảo đảm an toàn, ANTT.

2. Điều tra và xử lý các trường hợp vi phạm các quy định về an toàn, ANTT theo thẩm quyền và quy định hiện hành của Nhà nước.

Điều 17. Trách nhiệm của cán bộ, công chức, viên chức trong các cơ quan, đơn vị quản lý nhà nước

1. Trách nhiệm của cán bộ chuyên trách tại các cơ quan, đơn vị:

a) 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 cơ quan, 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.

b) 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.

c) Chịu trách nhiệm tham mưu chuyên môn và vận hành an toàn hệ thống thông tin của cơ quan, đơn vị theo nhiệm vụ được Thủ trưởng đơn vị phân công.

2. Trách nhiệm của cán bộ, công chức, viên chức trong các cơ quan, đơn vị quản lý nhà nước:

Nghiêm chỉnh thi hành các quy chế nội bộ, quy trình về an toàn, ANTT của cơ quan, 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.

Chương IV

TỔ CHỨC THỰC HIỆN

Điều 18. Tổ chức thực hiện

Sở Thông tin và Truyền thông chủ trì, phối hợp với các sở, ban ngành, Ủy ban

nhân dân các huyện, thành phố và các cơ quan, đơn vị có liên quan triển khai thực hiện Quy chế này.

Trong quá trình thực hiện, nếu có khó khăn, vướng mắc, các cơ quan, đơn vị kịp thời báo cáo về Sở Thông tin và Truyền thông để tổng hợp, trình Ủy ban nhân dân tỉnh xem xét, quyết định./.

TM. ỦY BAN NHÂN DÂN

KT. CHỦ TỊCH

PHÓ CHỦ TỊCH

Lê Quang Thích