ỦY BAN NHÂN DÂN TỈNH GIA LAI	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 41 /2016/QĐ-UBND	*Gia Lai, ngày 30 tháng 9 năm 2016*

QUYẾT ĐỊNH

V/v Ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Gia Lai

ỦY BAN NHÂN DÂN TỈNH

Căn cứ Luật Tổ chức chính quyền địa phương năm 2015;

Căn cứ Luật Ban hành văn bản quy phạm pháp luật năm 2015;

Căn cứ Luật Giao dịch điện tử năm 2005;

Căn cứ Luật Công nghệ thông tin năm 2006;

Căn cứ Luật An toàn thông tin mạng năm 2015;

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.

Xét đề nghị của Giám đốc Sở Thông tin và Truyền thông,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Gia Lai.

Điều 2. Quyết định có hiệu lực thi hành kể từ ngày 10 tháng 10 năm 2016.

Điều 3. Chánh Văn phòng Uỷ ban nhân dân tỉnh; Thủ trưởng các sở, ban, ngành; Chủ tịch Uỷ ban nhân dân các huyện, thị xã, thành phố và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Bộ Thông tin và Truyền thông;
- Thường trực Tỉnh ủy (báo cáo);
- Thường trực HĐND tỉnh;
- Cổng TTĐT Chính phủ;
- Cục Kiểm tra văn bản (Bộ Tư pháp);
- Ban Tuyên giáo Tỉnh ủy;
- Ban Nội chính Tỉnh ủy;
- Văn phòng Đoàn ĐBQH tỉnh;
- Văn phòng HĐND tỉnh;
- Sở Tư pháp;
- Các thành viên BCĐ UD CNTT tỉnh Gia Lai;
- Báo Gia Lai, Đài PT-TH tỉnh;
- Cổng TTĐT tỉnh Gia Lai;
- Lưu: VT, NC, KGVX.

TM. UỶ BAN NHÂN DÂN
CHỦ TỊCH

Võ Ngọc Thành

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

QUY CHẾ

Bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Gia Lai

(Ban hành kèm theo Quyết định số 41/2016/QĐ-UBND ngày 30 tháng 9 năm 2016 của Ủy ban nhân dân tỉnh Gia Lai)

Chương I

QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về công tác bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin (CNTT) của các cơ quan nhà nước tỉnh Gia Lai (*sau đây gọi tắt là các cơ quan, đơn vị*).

Điều 2. Đối tượng áp dụng

1. Quy chế này áp dụng đối với các cơ quan, đơn vị nhà nước và các đối tượng có liên quan trên địa bàn tỉnh Gia Lai, bao gồm:

a) Các Sở, ban, ngành;

b) Ủy ban nhân dân các huyện, thị xã, thành phố;

c) Ủy ban nhân dân các xã, phường, thị trấn;

d) Các đơn vị sự nghiệp công lập, các doanh nghiệp nhà nước trên địa bàn tỉnh.

2. Cán bộ, công chức, viên chức và người lao động đang làm việc tại các cơ quan, đơn vị quy định tại Khoản 1 Điều này.

3. Các tổ chức, cá nhân có liên quan 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.

Điều 3. Giải thích từ ngữ

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

1. Cán bộ được giao phụ trách bảo đảm an toàn thông tin mạng: Là cán bộ kỹ thuật hoặc cán bộ quản lý được giao phụ trách công tác bảo đảm an toàn thông tin cho việc triển khai, vận hành, khai thác hệ thống CNTT tại đơn vị.

2. Bên thứ ba: Là các tổ chức, cá nhân có chuyên môn về an toàn thông tin được các đơn vị thuê hoặc hợp tác nhằm cung cấp hàng hóa, dịch vụ kỹ thuật cho hệ thống CNTT.

3. Tài sản CNTT: Là các trang thiết bị, thông tin thuộc hệ thống CNTT của

cơ quan, đơn vị, bao gồm:

a) Tài sản vật lý: Là các thiết bị công nghệ thông tin, phương tiện truyền thông và các thiết bị khác gắn với hoạt động của hệ thống công nghệ thông tin, như: Máy vi tính, máy tính bảng, thiết bị lưu trữ, thiết bị ngoại vi, hệ thống điều hòa, hệ thống cung cấp điện, hệ thống chống sét, hệ thống quan sát...

b) Tài sản thông tin: Là các dữ liệu, tài liệu liên quan đến hệ thống công nghệ thông tin.

c) Tài sản phần mềm: Là các chương trình ứng dụng, phần mềm hệ thống, cơ sở dữ liệu và công cụ phát triển.

4. Máy chủ (Server): Là một máy tính được nối mạng, có IP tĩnh, có năng lực xử lý cao và trên máy đó được cài các phần mềm để phục vụ cho các máy PC khác truy cập để yêu cầu cung cấp dịch vụ và tài nguyên.

5. Tường lửa (Firewall): Là một thiết bị phần cứng hoặc phần mềm hoạt động trong môi trường máy tính nối mạng, là rào chắn mà một số cá nhân, tổ chức, doanh nghiệp, cơ quan nhà nước lập ra nhằm ngăn chặn người dùng từ bên ngoài truy nhập các thông tin bảo mật nằm trong mạng nội bộ.

6. Phần mềm độc hại (mã độc, Virus máy tính): Là những phần mềm hay đoạn mã được thiết kế để tự nhân bản và sao chép chính nó vào các đối tượng lây nhiễm khác (tập tin, ổ đĩa,..) Một số tên gọi như: Spyware, Worm, Trojan, ... tùy vào từng loại sẽ gây ảnh hưởng tới máy tính ở mức độ khác nhau.

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

1. Việc bảo đảm an toàn thông tin mạng là yêu cầu bắt buộc trong quá trình thiết kế, xây dựng, vận hành, nâng cấp, sử dụng và hủy bỏ trong ứng dụng CNTT của cơ quan nhà nước.

2. Việc thực hiện các phương pháp bảo đảm an toàn thông tin phải tuân theo quy định của Luật An toàn thông tin mạng, Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về việc bảo đảm an toàn hệ thống thông tin theo cấp độ và quy định của pháp luật có liên quan.

3. Thủ trưởng các cơ quan, đơn vị là người chịu trách nhiệm trực tiếp chỉ đạo công tác bảo đảm an toàn thông tin mạng.

4. Xác định rõ quyền hạn, trách nhiệm của Thủ trưởng, các phòng, ban và từng cá nhân trong cơ quan, đơn vị đối với công tác bảo đảm an toàn thông tin mạng.

5. Bố trí nguồn lực phù hợp với quy mô, điều kiện của cơ quan, đơn vị nhằm thực hiện tốt nhất công tác bảo đảm an toàn thông tin mạng.

6. Những văn bản có chứa nội dung bí mật nhà nước phải được quản lý theo chế độ mật theo quy định của pháp luật hiện hành. Không được truyền tải trên mạng nếu chưa có sự đồng ý của Thủ trưởng các cơ quan, đơn vị và phải được mã hóa theo quy định của Luật Cơ yếu.

7. Các cơ quan, đơn vị phải bố trí máy tính riêng, nghiêm cấm hành vi sử

dụng máy tính có kết nối Internet, mạng nội bộ (LAN) hay các thiết bị thông minh để soạn thảo văn bản có nội dung bí mật nhà nước.

8. Hoạt động bảo đảm an toàn thông tin mạng phải được thực hiện thường xuyên, liên tục, hiệu quả trên cơ sở tuân thủ tiêu chuẩn, quy chuẩn, quy định về an toàn thông tin mạng.

Chương II

QUY ĐỊNH BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 5. Quản lý tài sản công nghệ thông tin (CNTT)

1. Các cơ quan, đơn vị phải thống kê, kiểm kê tài sản CNTT (tài sản vật lý, tài sản thông tin, tài sản phần mềm) tối thiểu mỗi năm 01 lần.

2. Các cơ quan, đơn vị có trách nhiệm kiểm tra, đánh giá mức độ an toàn đối với các tài sản CNTT trước khi đưa vào sử dụng.

3. 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...) cần được lưu trữ, quản lý và cập nhật kịp thời.

4. Gắn quyền sử dụng tài sản cho các cá nhân hoặc bộ phận cụ thể, người sử dụng tài sản CNTT phải tuân thủ các quy định về quản lý, sử dụng tài sản, bảo đảm tài sản được sử dụng đúng mục đích và an toàn.

5. Phải xây dựng kế hoạch kiểm tra, bảo dưỡng tài sản theo định kỳ. Trang thiết bị lưu trữ thông tin khi không sử dụng nữa cần phải được thanh lý, hủy bỏ đúng quy trình kỹ thuật; tránh lộ, lọt thông tin bí mật, mất dữ liệu và phải bảo đảm không thể phục hồi.

6. Khi bên thứ ba thực hiện việc cung cấp, bảo dưỡng, sửa chữa tài sản CNTT, các cơ quan, đơn vị, phải thực hiện việc quản lý bảo đảm an toàn thông tin mạng như sau:

a) Đánh giá về năng lực kỹ thuật, nhân sự, khả năng tài chính của bên thứ ba trước khi ký kết hợp đồng cung cấp hàng hóa, dịch vụ.

b) Xác định rõ trách nhiệm, quyền hạn và nghĩa vụ của các bên về bảo đảm an toàn thông tin mạng khi ký hợp đồng. Hợp đồng với bên thứ ba, phải bao gồm các điều khoản về việc xử lý khi có vi phạm quy chế an toàn thông tin và trách nhiệm phải bồi thường thiệt hại của bên thứ ba trong trường hợp có thiệt hại do hành vi vi phạm của bên thứ ba gây ra.

c) Chú ý đến các vấn đề về tính bí mật, tính toàn vẹn, tính sẵn sàng, tin cậy, hiệu năng tối đa, khả năng phục hồi sau thảm họa, phương tiện lưu trữ của hệ thống thông tin khi có sự tham gia của bên thứ ba.

d) Áp dụng các biện pháp giám sát chặt chẽ và giới hạn quyền truy cập của bên thứ ba khi cho phép truy cập vào hệ thống CNTT của đơn vị.

Điều 6. Quản lý cán bộ, công chức, viên chức và người lao động

1. Các cơ quan, đơn vị phải thường xuyên tổ chức quán triệt các quy định về an toàn thông tin mạng, nhằm nâng cao nhận thức về trách nhiệm bảo đảm an toàn thông tin mạng của từng cá nhân trong cơ quan.

2. Cán bộ, công chức, viên chức, người lao động phải nghiêm túc tuân thủ thực hiện các quy chế bảo đảm an toàn thông tin mạng của cơ quan, đơn vị mình.

3. Cần phải bố trí nhân sự có năng lực và đạo đức đảm nhận vị trí phụ trách cho công tác bảo đảm an toàn thông tin mạng, quản trị hệ thống CNTT của cơ quan, đơn vị.

4. Các cơ quan, đơn vị phải xây dựng các yêu cầu, trách nhiệm bảo đảm an toàn thông tin mạng đối với từng vị trí công việc. Trước khi tiếp nhận nhân sự, các cơ quan, đơn vị phải kiểm tra khả năng đáp ứng các yêu cầu về an toàn thông tin mạng của nhân sự mới. Trong các hợp đồng lao động, phải có các điều khoản về trách nhiệm bảo đảm an toàn thông tin mạng.

5. Các cơ quan, đơn vị phải tạo điều kiện, lập kế hoạch đào tạo cho cán bộ, công chức, viên chức và người lao động để nâng cao kiến thức cơ bản và kỹ năng an toàn thông tin mạng; đồng thời phổ biến, cập nhật các quy chế về an toàn thông tin hàng năm để mọi người hiểu rõ các quyền và trách nhiệm đối với việc bảo đảm an toàn thông tin mạng. Thường xuyên kiểm tra việc thực hiện các nội quy, quy chế về an toàn thông tin mạng của đơn vị đối với cán bộ, công chức, viên chức, người lao động theo định kỳ.

6. Khi chấm dứt hoặc thay đổi công việc, các cơ quan, đơn vị phải: Xác định rõ trách nhiệm của cán bộ, công chức, viên chức, người lao động và các bên liên quan về hệ thống CNTT; Hủy tài khoản, quyền truy cập hoặc thay đổi quyền truy cập hệ thống CNTT (mật khẩu, chứng thư số, thư mục lưu trữ, thư điện tử, máy vi tính, thiết bị lưu trữ dùng chung...) cho phù hợp với công việc được thay đổi.

Điều 7. Quản lý, bảo đảm an toàn, an ninh hạ tầng ứng dụng CNTT

1. Đối với khu vực đặt trang thiết bị CNTT:

a) Các khu vực có yêu cầu cao về an toàn, bảo mật như phòng máy chủ, nơi đặt các thiết bị lưu trữ phải áp dụng biện pháp kiểm soát ra vào thích hợp, bảo đảm chỉ những người có nhiệm vụ mới được vào khu vực đó.

b) Bảo đảm an toàn môi trường vật lý (nhiệt độ, độ ẩm, ánh sáng,...) cho phòng máy chủ, các hệ thống hỗ trợ (máy điều hòa nhiệt độ, nguồn cấp điện, hệ thống chống sét, dự phòng nguồn điện, cáp quang truyền dẫn…) được an toàn và hoạt động ổn định, sẵn sàng.

c) Có nội quy, hướng dẫn làm việc trong các khu vực có lưu trữ thông tin cần bảo đảm an toàn, bảo mật.

2. Các cơ quan, đơn vị phải thực hiện các biện pháp bảo vệ cần thiết để phòng tránh mất cắp hoặc phá hoại tại các khu lắp đặt các thiết bị xử lý và lưu trữ của hệ thống thông tin, chỉ những người có quyền, nhiệm vụ mới được phép vào.

3. Chủ động thực hiện việc phân tích và đánh giá các mối đe dọa khách quan

như: Bão, lũ, cháy nổ, lở đất, vật liệu độc hại hoặc các mối đe dọa khác do thiên nhiên và có kế hoạch phòng chống.

4. Phải bố trí máy tính riêng đã được kiểm tra an ninh, không kết nối với mạng Internet và mạng nội bộ (LAN) nhằm tránh thất thoát thông tin khi soạn thảo các văn bản có nội dung bí mật nhà nước.

5. Hệ thống máy chủ (Servers) phải được dán nhãn, có sơ đồ đấu nối, thể hiện cụ thể về địa chỉ IP, tên máy chủ. Sơ đồ đấu nối phải được cập nhật nếu có sự thay đổi.

6. Ứng dụng chữ ký số chuyên dùng để bảo đảm an toàn thông tin mạng trong việc triển khai ứng dụng CNTT trong hoạt động cơ quan nhà nước và phục vụ công dân, tổ chức.

7. Về việc tổ chức mô hình mạng: Cài đặt, cấu hình, tổ chức hệ thống mạng theo mô hình mạng phân lớp, hạn chế sử dụng mô hình mạng ngang hàng. Các đơn vị có nhiều phòng, ban, đơn vị trực thuộc không nằm trong cùng một khu vực, cần thiết lập hệ thống mạng riêng bảo mật để bảo đảm an ninh cho mạng nội bộ.

8. Về việc quản lý hệ thống mạng không dây (Wifi): Khi thiết lập mạng không dây cho phép các thiết bị kết nối với mạng cục bộ qua hình thức không dây tại các điểm truy nhập, điểm đấu nối của thiết bị không dây vào mạng nội bộ cần ở lớp ngoài của mạng (mạng không dây cần thiết lập dãy địa chỉ khác lớp dãy địa chỉ của mạng nội bộ), thiết bị không dây cần được thiết lập các tham số như: tên, mật khẩu, mã hóa dữ liệu... và thường xuyên thay đổi mật khẩu nhằm tăng cường công tác bảo mật.

9. Chống mã độc, virus và các hình thức xâm nhập khác: Các cán bộ, công chức viên chức và người lao động trong cơ quan phải được hướng dẫn về phòng chống mã độc, các rủi ro do mã độc gây ra; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm trên máy trạm khi chưa có sự đồng ý của người có thẩm quyền theo quy định của cơ quan; Tất cả các máy tính của đơn vị phải được cấu hình nhằm vô hiệu hóa tính năng tự động thực thi (autoplay) các tập tin trên các thiết bị lưu trữ di động; tất cả các tập tin, thư mục phải được quét mã độc trước khi sao chép, sử dụng. Lựa chọn, triển khai các thiết bị phần cứng và phần mềm chống, phát hiện xâm nhập (IPS, IDS), phần mềm chống virus, mã độc có hiệu quả trên các máy chủ, máy trạm, các thiết bị, phương tiện kỹ thuật trong mạng, bảo vệ các hệ thống thông tin quan trọng như: Cổng/trang thông tin điện tử; hộp thư điện tử công vụ; một cửa điện tử; quản lý văn bản và điều hành; Hội nghị truyền hình qua mạng ... đồng thời, thường xuyên cập nhật phiên bản mới, bản vá lỗi của các phần mềm hệ thống, phần mềm chống xâm nhập, chống virus… nhằm kịp thời phát hiện, loại trừ mã độc máy tính.

10. Thiết bị có chứa thông tin mật, quan trọng của cơ quan, đơn vị trước khi mang đi bảo hành, bảo dưỡng, sửa chữa ở ngoài phạm vi cơ quan phải được sự đồng ý của người đứng đầu cơ quan, phải tháo thiết bị lưu trữ dữ liệu hoặc xóa hết dữ liệu đã lưu trữ trong thiết bị (theo phương pháp không thể phục hồi) và thực hiện các biện pháp theo các quy định về bảo vệ bí mật nhà nước.

Điều 8. Bảo đảm an toàn thông tin mạng trong quá trình vận hành, khai thác sử dụng các hệ thống thông tin

1. Tùy theo tình hình thực tế triển khai ứng dụng CNTT, các đơn vị cần thực hiện việc quản lý và kiểm soát mạng nhằm ngăn ngừa các hiểm họa và duy trì an toàn cho các hệ thống thông tin, phần mềm ứng dụng sử dụng mạng. Các nội dung có thể bao gồm:

a) Sử dụng thiết bị tường lửa, thiết bị phát hiện, ngăn chặn xâm nhập trái phép và các trang thiết bị khác nhằm bảo đảm an toàn bảo mật mạng.

b) Thiết lập, cấu hình đầy đủ các tính năng của thiết bị an ninh mạng.

c) Sử dụng các công cụ để dò tìm và phát hiện kịp thời các điểm yếu, lỗ hổng và các truy cập bất hợp pháp vào hệ thống mạng.

d) Thường xuyên kiểm tra, phát hiện những kết nối, trang thiết bị, phần mềm cài đặt bất hợp pháp vào hệ thống mạng.

2. Quản lý bản ghi nhật ký hệ thống: Hệ thống thông tin cần ghi nhận đầy đủ thông tin trong các bản ghi nhật ký khi thao tác trên hệ thống và lưu giữ nội dung nhật ký trong khoảng thời gian nhất định, để phục vụ việc quản lý, kiểm soát hệ thống thông tin. Thường xuyên thực hiện việc theo dõi bản ghi nhật ký hệ thống và các sự kiện khác có liên quan để đánh giá, báo cáo các rủi ro và mức độ nghiêm trọng các rủi ro đó. Các rủi ro có thể xảy ra do sự truy cập trái phép, sử dụng trái phép, xóa mất, thay đổi hoặc phá hủy thông tin và hệ thống thông tin.

3. Quản lý đăng nhập hệ thống: Các hệ thống thông tin cần giới hạn một số hữu hạn lần đăng nhập sai liên tiếp. Tổ chức theo dõi, và kiểm soát tất cả các phương pháp truy nhập từ xa tới hệ thống thông tin; yêu cầu người dùng đặt mật khẩu với độ an toàn cao.

4. Tổ chức quản lý tài nguyên: Kiểm tra, giám sát chức năng chia sẻ thông tin. Tổ chức cấp phát tài nguyên trên máy chủ theo danh mục thư mục cho từng phòng/ban; khuyến cáo người sử dụng cân nhắc việc chia sẻ tài nguyên thông tin trên máy đang sử dụng, khi thực hiện việc chia sẻ tài nguyên nếu cần thiết phải sử dụng mật khẩu để bảo vệ thông tin.

5. Khai thác, sử dụng các ứng dụng, hệ thống thông tin theo đúng chức năng, nhiệm vụ được giao, bảo đảm phục vụ tốt công tác chuyên môn, nghiệp vụ của đơn vị, phục vụ công dân, doanh nghiệp.

6. Trong quá trình vận hành hệ thống cần thực hiện quy định về phòng chống virus, mã độc đáp ứng các yêu cầu cơ bản như: Kiểm tra, diệt virus và mã độc trên các phương tiện mạng thông tin, dữ liệu nhận từ bên ngoài trước khi sử dụng; không mở các thư điện tử lạ, các tập tin đính kèm hoặc các liên kết trong các thư lạ để tránh virus, mã độc; không vào các trang thông tin điện tử hoặc mở các email (thư điện tử) không rõ nguồn gốc xuất xứ, đáng ngờ; không tải các trò chơi vào máy hoạt động công vụ; không tự ý cài đặt các phần mềm không rõ nguồn gốc, không có bản quyền; trong trường hợp phát hiện nhưng không diệt được virus, mã độc thì cần phải tắt nguồn điện vào thiết bị và báo ngay cho người quản

trị hệ thống xử lý.

Điều 9. Quản lý, khắc phục sự cố, lưu trữ và dự phòng

1. Các sự kiện, sự cố về an toàn thông tin mạng dưới đây cần được xem xét phân loại và xử lý theo Khoản 2, 3 của Điều này, bao gồm:

a) Những truy cập trái phép, hành vi vi phạm tính bảo mật và tính toàn vẹn dữ liệu, ứng dụng;

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

c) Phát hiện ra điểm yếu, lỗ hổng bảo mật của hạ tầng, hệ điều hành, ứng dụng;

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

đ) Mất thiết bị, phương tiện công nghệ thông tin;

e) Không tuân thủ chính sách an toàn thông tin hoặc các chỉ dẫn bắt buộc của đơn vị hoặc hành vi vi phạm an ninh vật lý;

g) Các trục trặc của phần mềm hay phần cứng không khắc phục được gây ảnh hưởng đến hoạt động của hệ thống CNTT;

h) Các sự cố khác gây gián đoạn, ảnh hưởng đến hoạt động bình thường của các ứng dụng CNTT tại đơn vị.

2. Cơ quan, đơn vị cần phân loại mức độ nghiêm trọng của các sự cố, bao gồm:

a) Thấp: Sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của cơ quan;

b) Trung bình: Sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hay đình trệ hoạt động chính của đơn vị;

c) Cao: Sự cố làm cho thiết bị, phần mềm hay hệ thống không thể sử dụng được và gây ảnh hưởng đến hoạt động chung của cơ quan;

d) Khẩn cấp: Sự cố ảnh hưởng đến sự liên tục của nhiều hoạt động chính của cơ quan.

3. Khi có sự cố hoặc nguy cơ mất an toàn thông tin mạng thì lãnh đạo đơn vị phải chỉ đạo kịp thời:

a) Áp dụng mọi biện pháp để khắc phục và hạn chế thiệt hại do sự cố xảy ra, lập biên bản báo cáo cho cơ quan cấp trên quản lý trực tiếp;

b) Trường hợp có sự cố nghiêm trọng ở mức độ cao, khẩn cấp hoặc vượt quá khả năng khắc phục của cơ quan, đơn vị, lãnh đạo cơ quan, đơn vị phải báo cáo ngay cho Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ;

c) Tạo điều kiện thuận lợi cho cơ quan chức năng tham gia khắc phục sự cố và thực hiện theo đúng hướng dẫn;

d) Báo cáo bằng văn bản về sự cố cho cơ quan cấp trên quản lý trực tiếp và

Sở Thông tin và Truyền thông.

4. Tất cả cán bộ, công chức, viên chức, người lao động và bên thứ ba khi phát hiện các sự cố về an toàn thông tin mạng của đơn vị cần thực hiện việc báo cáo với cấp trên và bộ phận phụ trách công nghệ thông tin của cơ quan, đơn vị đó để kịp thời ngăn chặn và xử lý kịp thời.

5. Thiết lập cơ chế sao lưu và phục hồi hệ thống:

a) Các dữ liệu quan trọng của cơ quan phải được sao lưu, bao gồm: thông tin cấu hình của hệ thống mạng, máy chủ; cơ sở dữ liệu của các phần mềm ứng dụng (quản lý văn bản và điều hành, một cửa điện tử, cổng/trang thông tin điện tử, thư điện tử công vụ...); tập tin ghi nhật ký.

b) Ban hành và thực hiện quy trình sao lưu dự phòng và phục hồi dữ liệu cho các phần mềm, dữ liệu cần thiết khi gặp sự cố;

c) 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 phục hồi hệ thống từ dữ liệu sao lưu;

d) Dữ liệu sao lưu phải được lưu trữ an toàn và được kiểm tra thường xuyên bảo đảm sẵn sàng cho việc sử dụng khi cần.

e) Thực hiện sao lưu dữ liệu định kỳ trên các máy chủ của cơ quan, đơn vị và tất cả các máy tính trang bị cho cán bộ, công chức, viên chức và người lao động. Dữ liệu phải được sao lưu ra thiết bị lưu trữ ngoài (như ổ cứng di động, thiết bị lưu trữ ngoài...) nhằm bảo đảm tính an toàn và thuận tiện cho quá trình phục hồi dữ liệu khi gặp sự cố.

Điều 10. Bảo đảm an toàn thông tin mạng các hệ thống thông tin, ứng dụng, cơ sở hạ tầng dùng chung, tích hợp ứng dụng và chia sẻ dữ liệu

1. Trong quá trình khai thác, vận hành và sử dụng các ứng dụng, cơ sở hạ tầng dùng chung, các cơ quan, đơn vị tham gia phải tuân thủ các quy chế về bảo đảm an toàn thông tin mạng theo yêu cầu của từng hệ thống, ứng dụng, đặc biệt là các hệ thống, phần mềm, hạ tầng dùng chung của tỉnh, bao gồm:

a) Khai thác mạng tin học diện rộng của tỉnh (WAN);

b) Sử dụng và vận hành Trung tâm tích hợp dữ liệu của tỉnh;

c) Khai thác sử dụng hệ thống thư điện tử công vụ;

d) Các Trang/cổng thông tin điện tử, các phần mềm dùng chung: Quản lý văn bản và điều hành và Trục liên thông văn bản điện tử, một cửa điện tử...;

đ) Hệ thống Hội nghị truyền hình qua mạng.

2. Trong quá trình triển khai việc tích hợp các hệ thống, phần mềm ứng dụng, chia sẻ dữ liệu, cần triển khai các giải pháp bảo đảm an toàn thông tin mạng cho từng hệ thống, phần mềm ứng dụng và trong quá trình chia sẻ dữ liệu cũng như làm rõ trách nhiệm của từng cơ quan, đơn vị, từng cá nhân tham gia vào hệ thống.

Điều 11. Ban hành và triển khai quy chế bảo đảm an toàn thông tin mạng tại cơ quan, đơn vị

1. Các cơ quan, đơn vị phải xây dựng quy chế nội bộ bảo đảm an toàn, an ninh cho hệ thống thông tin, trong đó bao gồm tối thiểu các nội dung sau:

a) Yêu cầu và nguyên tắc của công tác bảo đảm an toàn, an ninh;

b) Yêu cầu về quản lý tài sản CNTT của cơ quan, đơn vị;

c) Yêu cầu về quản lý về cán bộ, công chức, viên chức và người lao động khi tham gia vào hệ thống CNTT và viễn thông của cơ quan, đơn vị;

d) Yêu cầu về quản lý, bảo đảm an toàn môi trường mạng;

đ) Yêu cầu về bảo đảm an toàn vận hành các hệ thống thông tin;

e) Quản lý sự cố, lưu trữ và dự phòng;

g) Phân công trách nhiệm và tổ chức thực hiện.

2. Các cơ quan, đơn vị phải tổ chức giám sát việc thực hiện quy chế bảo đảm an toàn thông tin mạng cho hệ thống thông tin sau khi được ban hành.

3. Định kỳ 6 tháng, 1 năm phải có kiểm tra, sơ kết việc thực hiện Quy chế bảo đảm an toàn thông tin mạng và kết hợp vào báo cáo tình hình ứng dụng CNTT tại cơ quan, đơn vị gửi Sở Thông tin và Truyền thông để tổng hợp báo cáo với Ủy ban nhân dân tỉnh, Bộ Thông tin và Truyền thông.

Chương III

TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 12. Trách nhiệm của cán bộ, công chức, viên chức và người lao động trong các cơ quan, đơn vị

1. Trách nhiệm của cán bộ, công chức, viên chức và người lao động được giao phụ trách an toàn thông tin mạng:

a) Chịu trách nhiệm bảo đảm an toàn thông tin mạng của cơ quan, đơn vị;

b) Tham mưu lãnh đạo cơ quan ban hành các quy chế, quy trình nội bộ, triển khai các giải pháp kỹ thuật bảo đảm an toàn thông tin mạng;

c) Thực hiện việc giám sát, đánh giá, báo cáo Thủ trưởng cơ quan, đơn vị các rủi ro mất an toàn thông tin mạng và mức độ nghiêm trọng của các rủi ro đó;

d) Phối hợp với các cá nhân, đơn vị có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn thông tin mạng;

đ) Thường xuyên cập nhật nâng cao kiến thức, trình độ chuyên môn đáp ứng yêu cầu bảo đảm an toàn thông tin mạng của đơn vị.

2. Trách nhiệm của cán bộ, công chức, viên chức, người lao động trong các cơ quan, đơn vị:

a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông

tin mạng trong phạm vi trách nhiệm và quyền hạn được giao;

b) Mỗi cán bộ, công chức, viên chức và người lao động phải có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng;

c) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách công nghệ thông tin của cơ quan, đơn vị để kịp thời ngăn chặn và xử lý;

d) Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng được tỉnh hoặc đơn vị chuyên môn tổ chức.

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

1. Thủ trưởng các cơ quan, đơn vị có trách nhiệm tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trong công tác bảo đảm an toàn thông tin mạng của cơ quan, đơn vị mình.

2. Phân công một bộ phận hoặc cán bộ phụ trách bảo đảm an toàn thông tin mạng của đơn vị, tạo điều kiện để các cán bộ được học tập, nâng cao trình độ về an toàn thông tin mạng.

3. Bố trí, tạo điều kiện làm việc cho cán bộ chuyên trách về công nghệ thông tin trong các cơ quan, đơn vị phù hợp với chuyên môn, được ưu tiên bồi dưỡng nghiệp vụ về an toàn thông tin mạng.

4. Xây dựng quy chế, quy trình về bảo đảm an toàn thông tin mạng phù hợp với Quy chế này và các quy định của pháp luật.

5. Phối hợp, cung cấp thông tin và tạo điều kiện cho các đơn vị có thẩm quyền triển khai công tác kiểm tra khắc phục sự cố xảy ra một cách kịp thời, nhanh chóng và đạt hiệu quả.

6. Phối hợp chặt chẽ với Sở Thông tin và Truyền thông, Công an tỉnh trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin mạng.

7. Khuyến khích các cơ quan, đơn vị liên kết các tổ chức, cá nhân, doanh nghiệp CNTT mở các khóa đào tạo nhân lực trong lĩnh vực an toàn thông tin mạng mạng.

8. Hàng năm bố trí kinh phí cho việc ứng dụng công nghệ thông tin nói chung và công tác bảo đảm an toàn thông tin mạng nói riêng trong nội bộ cơ quan, đơn vị mình; lập kế hoạch nâng cấp, bảo trì, sửa chữa, gia hạn bản quyền phần mềm... cho các hệ thống phần cứng, phần mềm nhằm thực hiện tốt công tác bảo mật, bảo đảm an toàn thông tin mạng đưa vào dự toán chi năm sau để triển khai thực hiện.

Điều 14. Trách nhiệm của Sở Thông tin và Truyền thông

1. Tham mưu Ủy ban nhân dân tỉnh và Ban chỉ đạo ứng dụng CNTT của tỉnh về công tác bảo đảm an toàn thông tin mạng trên địa bàn tỉnh.

2. Làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an

toàn thông tin mạng trên địa bàn tỉnh.

3. 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 thông tin mạng định kỳ hàng năm hoặc theo chỉ đạo của UBND tỉnh đối với các cơ quan nhà nước trong tỉnh.

4. 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 an toàn thông tin mạng.

5. Tổng hợp và báo cáo về tình hình an toàn thông tin mạng theo định kỳ cho Bộ Thông tin và Truyền thông, Ủy ban nhân dân tỉnh theo quy định của pháp luật.

6. Hàng năm, xây dựng và triển khai các chương trình đào tạo, tập huấn về công tác bảo đảm an toàn thông tin mạng cho cán bộ, công chức phụ trách an toàn thông tin mạng của các cơ quan, đơn vị. Tổ chức các hội nghị, hội thảo chuyên đề và tuyên truyền về an toàn thông tin mạng trong công tác quản lý nhà nước trên địa bàn tỉnh.

7. Tổ chức tuyên truyền, hướng dẫn về công tác bảo đảm an toàn thông tin mạng.

8. Phối hợp với Ban Tuyên giáo Tỉnh ủy, Công an tỉnh có các biện pháp phòng, chống các thông tin vi phạm pháp luật, ảnh hưởng đến an ninh quốc gia, trật tự, an toàn xã hội trên môi trường mạng, nhất là trên các cổng/trang thông tin điện tử, mạng xã hội.

Điều 15. Trách nhiệm của Công an tỉnh

1. Chủ trì, phối hợp với Sở Thông tin và Truyền thông và các đơn vị có liên quan hướng dẫn thực hiện văn bản quy phạm pháp luật về bảo vệ bí mật nhà nước.

2. Thực hiện công tác quản lý giám sát an toàn thông tin mạng trong Công an tỉnh.

3. Tổ chức, chỉ đạo, triển khai công tác phòng, chống, điều tra tội phạm lợi dụng hệ thống mạng để xâm phạm an ninh quốc gia, trật tự an toàn xã hội.

4. Phối hợp với Sở Thông tin và Truyền thông kiểm tra, xử lý các vi phạm về an toàn thông tin mạng theo quy định.

5. Hỗ trợ các đơn vị đánh giá nguy cơ mất an toàn thông tin mạng khi có yêu cầu.

Chương IV

TỔ CHỨC THỰC HIỆN

Điều 16. Các cơ quan, đơn vị, tổ chức, cá nhân có thành tích trong việc bảo đảm an toàn thông tin mạng được khen thưởng theo quy định của pháp luật.

Điều 17. Các cơ quan, đơn vị, tổ chức, cá nhân có hành vi vi phạm các quy định về bảo đảm an toàn thông tin mạng, tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật, xử lý vi phạm hành chính hoặc truy cứu trách nhiệm hình sự theo các quy định của pháp luật hiện hành.

Điều 18. Ban Chỉ đạo Ứng dụng Công nghệ thông tin của tỉnh đưa việc bảo đảm an toàn thông tin mạng vào tiêu chí xếp hạng ứng dụng công nghệ thông tin hàng năm của tỉnh.

Điều 19. Thủ trưởng các Sở, ban, ngành, Chủ tịch Uỷ ban nhân dân các huyện, thị xã, thành phố tổ chức thực hiện Quy chế này. Định kỳ hàng năm hoặc đột xuất, báo cáo công tác bảo đảm an toàn thông tin mạng cho UBND tỉnh (thông qua Sở Thông tin và Truyền thông).

Điều 20. Sở Kế hoạch và Đầu tư, Sở Tài chính phối hợp Sở Thông tin và Truyền thông tham mưu UBND tỉnh bố trí kinh phí cho các hoạt động bảo đảm an toàn thông tin mạng trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh.

Điều 21. Trong quá trình thực hiện Quy chế, nếu có vấn đề vướng mắc, phát sinh, các đơn vị phản ánh kịp thời về Sở Thông tin và Truyền thông để tổng hợp báo cáo Uỷ ban nhân dân tỉnh điều chỉnh, bổ sung./.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Võ Ngọc Thành