ỦY BAN NHÂN DÂN TỈNH LÂM ĐỒNG	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 45 /QĐ-UBND	*Lâm Đồng, ngày 11 tháng 01 năm 2016*

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 thuộc tỉnh Lâm Đồng.

CHỦ TỊCH ỦY BAN NHÂN DÂN TỈNH LÂM ĐỒNG

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19 tháng 6 năm 2015;

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 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ về việc 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 quy định về việc quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng;

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, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan, đơn vị thuộc tỉnh Lâm Đồng.

Điều 2. Chánh Văn phòng Ủy ban nhân dân tỉnh; Giám đốc Sở Thông tin và Truyền thông; Chủ tịch Ủy ban nhân dân các huyện, thành phố Đà Lạt và Bảo Lộc; Thủ trưởng các cơ quan, đơn vị và các cá nhân liên quan chịu trách nhiệm thi hành Quyết định này kể từ ngày ký./.

Nơi nhận:
- TT TU, TT HĐND tỉnh;
- CT, các PCT UBND tỉnh;
- Như Điều 2;
- Đài PTTH tỉnh, Báo Lâm Đồng;
- Trung tâm Công báo tỉnh;
- Lưu: VT, VX_1.

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Phan Văn Đa

ỦY BAN NHÂN DÂN TỈNH LÂM ĐỒNG	CỘNG HOÀ 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 thuộc tỉnh Lâm Đồng.

(Ban hành kèm theo Quyết định số 45 /QĐ-UBND ngày 11 /01/2016 của Ủy ban nhân dân tỉnh Lâm Đồng)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. Quy chế này quy định về công tác đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước, đơn vị sự nghiệp thuộc tỉnh Lâm Đồng.

2. Quy chế này áp dụng đối với các cơ quan hành chính, các đơn vị sự nghiệp và Ủy ban nhân dân các huyện, thành phố thuộc tỉnh (sau đây gọi chung là cơ quan); cán bộ, công chức, viên chức và người lao động tham gia vận hành, khai thác và sử dụng hệ thống thông tin tại các cơ quan.

3. Khuyến khích các cơ quan của Trung ương, tỉnh, thành phố khác hoạt động trên địa bàn tỉnh Lâm Đồng áp dụng và tham gia thực hiện Quy chế này.

Điều 2. Mục đích, nguyên tắc đảm bảo an toàn thông tin

1. Việc áp dụng Quy chế này nhằm giảm thiểu các nguy cơ gây mất an toàn thông tin và đảm bảo an ninh thông tin trong quá trình ứng dụng công nghệ thông tin trong hoạt động của các cơ quan.

2. Các hoạt động ứng dụng công nghệ thông tin phải tuân theo nguyên tắc đảm bảo an toàn thông tin quy định tại Điều 41, 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; các tiêu chuẩn kỹ thuật quản lý an toàn trong bộ tiêu chuẩn TCVN 7562:2005 và ISO/IEC 17799:2005.

Điều 3. Giải thích từ ngữ

Trong Quy chế này, các từ ngữ được sử dụng có nghĩa như sau:

1. TCVN 7562:2005: Tiêu chuẩn Việt Nam về mã thực hành quản lý an toàn thông tin.

2. ISO/IEC 17799:2005: Tiêu chuẩn quốc tế cung cấp các hướng dẫn quản lý an toàn bảo mật thông tin dựa trên quy phạm công nghiệp tốt nhất.

3. Mirror: Cơ chế cài đặt một máy chủ dự phòng hoạt động song song với máy chủ chính có nhiệm vụ làm bản sao cho máy chủ chính, dự phòng trường hợp máy chủ chính gặp sự cố.

4. Raid: Cơ chế cho phép ghép nhiều ổ đĩa cứng vật lý thành một hệ thống ổ đĩa cứng có chức năng gia tăng tốc độ đọc/ghi dữ liệu và sự an toàn của dữ liệu chứa trên hệ thống đĩa.

5. Clustering: Cơ chế cho phép sử dụng nhiều máy chủ kết hợp với nhau tạo thành một cụm có khả năng chịu đựng hay chấp nhận sai sót nhằm nâng cao khả năng sẵn sàng cho các hệ thống mạng máy tính.

6. Log file: Tập tin được tạo ra bởi một thiết bị, hệ thống (máy chủ, phần mềm tường lửa,...) mà trong đó có chứa tất cả thông tin về lịch sử hoạt động trên thiết bị, hệ thống đó.

7. System Restore: Tính năng hệ thống tự tạo ra các điểm khôi phục của hệ thống, giúp người dùng có thể khôi phục lại trạng thái của hệ thống trở về một thời điểm nào đó, trước khi có sự cố xảy ra.

Chương II
QUY ĐỊNH ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 4. Quản lý cán bộ, công chức, viên chức và người lao động

1. Thủ trưởng các cơ quan thường xuyên tổ chức phổ biến, quán triệt các quy định về an toàn thông tin, nâng cao nhận thức và trách nhiệm đảm bảo an toàn thông tin của từng cá nhân trong cơ quan.

2. Hủy tài khoản, quyền truy cập các hệ thống thông tin, thu hồi tất cả các tài sản liên quan tới hệ thống thông tin (khoá, thẻ nhận dạng, thư mục lưu trữ, thư điện tử, máy vi tính, tài khoản người dùng hệ thống,...) đối với các cá nhân nghỉ việc, chuyển công tác.

Điều 5. Biện pháp quản lý kỹ thuật đảm bảo an toàn, an ninh thông tin

1. Tổ chức mô hình mạng:

a) Cài đặt, cấu hình, quản trị hệ thống mạng nội bộ theo mô hình Clients/Server để kiểm soát máy trạm, hạn chế sử dụng mô hình mạng ngang hàng. Các cơ quan có nhiều phòng, ban, đơn vị trực thuộc không trong cùng một khu vực, phải thiết lập mạng riêng ảo (Virtual Private Network - VPN) để đảm bảo an ninh cho mạng nội bộ, đồng thời, phải tuân thủ các chính sách về an toàn thông tin do Chính phủ, Bộ Thông tin và Truyền thông và UBND tỉnh ban hành khi kết nối với các hệ thống thông tin và mạng internet. Khi thiết lập dịch vụ trên môi trường mạng internet, chỉ cung cấp những chức năng thiết yếu đảm bảo 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.

b) Tùy điều kiện, yêu cầu thực tế về bảo mật dữ liệu, các cơ quan chủ động triển khai xây dựng mô hình, giải pháp an toàn bảo mật hệ thống mạng tại cơ quan cho phù hợp.

2. 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), cơ quan cung cấp dịch vụ phải thiết lập các tham số như tên, mật khẩu, mã hóa dữ liệu và thông báo các thông tin liên quan đến điểm truy nhập để cơ quan sử dụng, định kỳ 03 tháng thay đổi mật khẩu nhằm tăng cường công tác bảo mật.

3. Phòng máy chủ:

a) Phải độc lập, là khu vực hạn chế tiếp cận và được lắp đặt hệ thống camera giám sát. Chỉ những người có trách nhiệm mới được phép vào. Quá trình vào, ra phòng máy chủ phải được ghi nhận vào nhật ký quản lý.

b) Các thiết bị mạng quan trọng như tường lửa (firewall), thiết bị định tuyến (router), hệ thống máy chủ,... phải được đặt trong phòng máy chủ và có các biện pháp bảo vệ, ngăn chặn xâm nhập trái phép.

c) Phải có hệ thống lưu điện đủ công suất và duy trì được thời gian hoạt động của các máy chủ tối thiểu 30 phút khi xảy ra sự cố mất điện; phải trang bị hệ thống chống sét theo quy định.

4. Phòng chống mã độc:

a) Lựa chọn, triển khai các phần mềm chống mã độc, thư rác trên tất cả các máy trạm, máy chủ, thiết bị mạng, thiết bị di động trong mạng và các hệ thống thông tin xung yếu *(cổng thông tin điện tử, thư điện tử, một cửa điện tử,...)*. Thường xuyên cập nhật các phiên bản mới, các bản vá lỗi của các phần mềm chống mã độc mới nhất hoặc phải được thiết lập chế độ tự động cập nhật, chế độ tự động quét mã độc khi sao chép, mở các tập tin.

b) Cán bộ, công chức, viên chức và người lao động trong cơ quan phải được tập huấn, hướng dẫn về phòng chống mã độc; không tự ý cài đặt hoặc gỡ bỏ các phần mềm trên máy trạm khi chưa được sự đồng ý của người có thẩm quyền của cơ quan; quét mã độc tất cả các tập tin, thư mục trước khi sao chép, sử dụng.

c) Khi phát hiện bất kỳ dấu hiệu liên quan đến việc bị nhiễm mã độc trên máy trạm (*máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu,...*), người sử dụng phải tắt máy và báo trực tiếp cho bộ phận có trách nhiệm của cơ quan để xử lý.

5. Các biện pháp kỹ thuật với trang thông tin điện tử/cổng thông tin điện tử:

a) Các trang thông tin lưu trữ bên ngoài Cổng thông tin điện tử của tỉnh: Quản lý toàn bộ các phiên bản của mã nguồn, phối hợp với đơn vị thực hiện dịch vụ lưu trữ tổ chức mô hình trang web hợp lý, tránh khả năng tấn công. Yêu cầu đơn vị cung cấp dịch vụ lưu trữ web cài đặt các hệ thống phòng vệ như tường lửa (firewall), thiết bị phát hiện/phòng chống xâm nhập (IDS/IPS), mức ứng dụng web (WAF-Web Application Firewall); thường xuyên cập nhật bản vá lỗi mới nhất cho hệ quản trị cơ sở dữ liệu, gỡ bỏ các cơ sở dữ liệu không sử dụng; sao lưu toàn bộ nội dung trang web (*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 trong vòng 24 giờ.

b) Các trang thông tin lưu trữ trên Cổng thông tin điện tử của tỉnh: Việc đảm bảo an toàn an ninh thông tin, bảo đảm khi có sự cố có thể khắc phục lại ngay trong vòng 24 giờ đối với các trang thông tin điện tử thành viên do Trung tâm Quản lý Cổng thông tin điện tử của tỉnh chịu trách nhiệm. Việc bổ sung

hoặc thêm các nội dung, các chức năng, gỡ bỏ các cơ sở dữ liệu không sử dụng,... phải liên hệ với Trung tâm Quản lý Cổng thông tin điện tử của tỉnh để được hỗ trợ.

6. Quản lý chia sẻ tài nguyên:

Người sử dụng phải chịu trách nhiệm về việc chia sẻ tài nguyên cục bộ trên máy đang sử dụng (tuyệt đối không được chia sẻ toàn bộ ổ cứng); khi chia sẻ tài nguyên trên máy chủ phải đặt mật khẩu.

7. Thiết lập cơ chế sao lưu và phục hồi máy chủ, máy trạm:

a) Các cơ quan phải lập kế hoạch và thực hiện sao lưu dữ liệu phù hợp với điều kiện của cơ quan, đảm bảo khả năng phục hồi dữ liệu khi có sự cố xảy ra.

b) Đối với máy trạm: Thực hiện việc sao lưu dữ liệu như hệ điều hành, các phần mềm ứng dụng văn phòng, phần mềm chuyên ngành, cơ sở dữ liệu, tập tin ghi nhật ký,... Sau khi sao lưu mỗi máy phải được lưu vào các thiết bị lưu trữ như: đĩa CD, ổ cứng ngoài, ... và thực hiện đánh số, dán nhãn giúp phục hồi dữ liệu được nhanh nhất.

c) 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.

8. Quản lý thiết bị tường lửa:

a) Các hạ tầng công nghệ thông tin phải được trang bị tường lửa, hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS) để phát hiện và ngăn chặn các xâm nhập trái phép vào mạng nội bộ.

b) Nhật ký hoạt động của thiết bị tường lửa phải được lưu giữ an toàn để phục vụ công tác khảo sát, điều tra khi có sự cố xảy ra.

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

a) Hệ thống thông tin cần ghi nhận: Quá trình đăng nhập vào hệ thống, các thao tác cấu hình hệ thống; các hành vi xem, thiết lập cấu hình hệ thống; việc thiết lập các kết nối bất thường vào, ra hệ thống; thay đổi quyền truy cập hệ thống. Thường xuyên kiểm tra, sao lưu các tập tin ghi (log file) theo từng tháng để lưu vết theo dõi, xác định những sự kiện đã xảy ra của hệ thống và hạn chế việc tràn tập tin ghi gây ảnh hưởng đến hoạt động của hệ thống.

b) 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.

c) Thường xuyên thực hiện việc theo dõi bản ghi nhật ký của 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.

10. Quản lý truy cập:

a) Các quy định về quản lý truy cập vào hệ thống thông tin, mạng máy tính, thiết bị, phần mềm ứng dụng phải được quy định chi tiết và tổ chức thực hiện nghiêm túc, phù hợp với các quy định của pháp luật về an toàn thông tin.

b) Mỗi tài khoản truy cập các hệ thống thông tin chỉ được cấp cho một người quản lý và sử dụng.

c) Mỗi cán bộ, công chức, viên chức và người lao động chỉ được phép truy cập các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình, có trách nhiệm bảo mật tài khoản truy cập thông tin.

d) Hệ thống thông tin tại các cơ quan phải có cơ chế giới hạn số lần đăng nhập sai liên tiếp. Nếu liên tục đăng nhập sai vượt quá số lần quy định thì hệ thống sẽ tự động khóa hoặc cô lập tài khoản trong một khoảng thời gian nhất định trước khi tiếp tục cho đăng nhập.

đ) Cán bộ chuyên trách có trách nhiệm theo dõi và kiểm soát tất cả các phương pháp truy cập từ xa (quay số, Internet...) tới hệ thống thông tin, bao gồm cả sự truy cập có chức năng đặc quyền. Hệ thống thông tin tại các cơ quan phải có cơ chế kiểm tra, cho phép tương ứng với mỗi phương pháp truy cập từ xa và cơ chế tự động giám sát, điều khiển các truy cập từ xa.

e) Các tài khoản người dùng liên quan đến hệ thống công nghệ thông tin của cơ quan phải được đặt mật khẩu truy cập. Mật khẩu đăng nhập vào các hệ thống thông tin phải có độ phức tạp cao (độ dài tối thiểu 8 ký tự, có ký tự viết hoa, ký tự số và ký tự đặc biệt như !, @, #, $, %,...) và phải được thay đổi ít nhất 3 tháng/lần.

Điều 6. Các hành vi bị nghiêm cấm

1. Tạo, cài đặt, phát tán vi rút máy tính, phần mềm độc hại trái pháp luật.

2. Xâm nhập, sửa đổi, xóa nội dung thông tin của cơ quan, cá nhân khác.

3. Cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin.

4. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của cơ quan, cá nhân khác trên môi trường mạng.

5. Hành vi khác làm mất an toàn, bí mật thông tin của cơ quan, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 7. Trách nhiệm của các cơ quan

1. Thủ trưởng các cơ quan chịu trách nhiệm toàn diện trước Ủy ban nhân dân tỉnh trong công tác đảm bảo an toàn, an ninh cho hệ thống thông tin của đơn vị, đồng thời thực hiện nghiêm túc các quy định tại Quy chế này.

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

3. Khi có sự cố hoặc nguy cơ mất an toàn, an ninh thông tin, kịp thời áp dụng mọi biện pháp để khắc phục và hạn chế thiệt hại, ưu tiên sử dụng lực lượng kỹ thuật an toàn thông tin của đơn vị, lập biên bản, báo cáo bằng văn bản cho cơ quan cấp trên quản lý trực tiếp và Sở Thông tin và Truyền thông.

4. 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.

5. Báo cáo tình hình và kết quả thực hiện công tác đảm bảo an toàn, an ninh thông tin tại cơ quan và gửi về Sở Thông tin và Truyền thông định kỳ mỗi năm 01 lần vào cuối quý IV.

Điều 8. Trách nhiệm của Sở Thông tin và Truyền thông

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

2. Xây dựng kế hoạch, dự toán kinh phí triển khai công tác an toàn và an ninh thông tin phục vụ vận hành các hệ thống thông tin được Ủy ban nhân dân tỉnh giao quản lý và các trang thông tin điện tử của các đơn vị.

3. Chủ trì, phối hợp với Công an tỉnh và các cơ quan liên quan tổ chức kiểm tra định kỳ hoặc đột xuất; kịp thời phát hiện và xử lý theo quy định của pháp luật đối với các cơ quan, tổ chức, cá nhân có các dấu hiệu, hành vi vi phạm an toàn, an ninh thông tin trên địa bàn tỉnh.

4. Tùy theo mức độ sự cố, phối hợp với 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, an ninh thông tin.

5. Tổ chức, phối hợp tổ chức tuyên truyền, phổ biến, cập nhật kiến thức về đảm bảo an toàn, an ninh thông tin cho người lao động trong các cơ quan thuộc tỉnh.

6. Hướng dẫn, giám sát các cơ quan trên địa bàn tỉnh xây dựng quy chế đảm bảo an toàn, an ninh cho hệ thống thông tin theo quy định.

7. Định kỳ tổng hợp, báo cáo Bộ Thông tin và Truyền thông, Ủy ban nhân dân tỉnh và các cơ quan liên quan về tình hình đảm bảo an toàn, an ninh thông tin trên địa bàn tỉnh.

Điều 9. Trách nhiệm của Công an tỉnh

1. Chủ trì, phối hợp với Sở Thông tin và Truyền thông và các cơ quan liên quan xây dựng kế hoạch đảm bảo an ninh mạng trên địa bàn tỉnh và kiểm soát, phòng ngừa, đấu tranh, ngăn chặn các loại tội phạm sử dụng công nghệ cao gây hại đến an toàn, an ninh thông tin trong cơ quan nhà nước.

2. Phối hợp với các cơ quan chức năng trong trao đổi biện pháp kỹ thuật, kiểm tra, đánh giá nhằm đảm bảo an toàn, an ninh thông tin.

3. Tăng cường công tác phòng ngừa, phát hiện và tuyên truyền, phổ biến pháp luật về xử lý tội phạm trong việc đảm bảo an toàn, an ninh thông tin.

4. Điều tra và xử lý các trường hợp vi phạm pháp luật về an toàn, an ninh thông tin theo thẩm quyền.

5. Thực hiện nhiệm vụ bảo vệ an toàn các công trình quan trọng về an ninh quốc gia trên lĩnh vực công nghệ thông tin.

Điều 10. Trách nhiệm của cán bộ, công chức, viên chức và người lao động trong các cơ quan

1. Trách nhiệm của người phụ trách an toàn thông tin:

a) Đảm bảo an toàn thông tin của cơ quan, triển khai các biện pháp quản lý vận hành, quản lý kỹ thuật và tham mưu xây dựng các quy định đảm bảo an toàn, an ninh thông tin cho hệ thống thông tin tại đơn vị theo các quy định của Quy chế này.

b) Tham mưu chuyên môn và vận hành an toàn hệ thống thông tin của cơ quan theo nhiệm vụ được phân công.

c) Giám sát, đánh giá, báo cáo thủ trưởng cơ quan các rủi ro, mất an toàn thông tin 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, an ninh thông tin.

2. Trách nhiệm của cán bộ, công chức, viên chức và người lao động:

a) Nghiêm chỉnh thi hành các quy chế, quy trình an toàn, an ninh thông tin của cơ quan và các quy định khác của pháp luật, nâng cao ý thức cảnh giác, trách nhiệm đảm bảo an toàn, an ninh thông tin tại cơ quan.

b) Quản lý, bảo quản thiết bị được giao sử dụng; không tự ý thay đổi, tháo lắp các thiết bị trên máy tính; không vào các trang web không rõ nội dung; không tải và cài đặt các phần mềm không rõ nguồn gốc, không liên quan đến công việc chuyên môn; quét mã độc tất cả các tập tin, thư mục trước khi sao chép, sử dụng.

c) Khi phát hiện sự cố phải báo ngay với cấp trên và bộ phận chuyên trách để kịp thời ngăn chặn, xử lý.

d) Thường xuyên cập nhật kiến thức về đảm bảo an ninh, an toàn thông tin.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 11. Khen thưởng và xử lý vi phạm

1. Hằng năm, Sở Thông tin và Truyền thông dựa trên kết quả kiểm tra, đánh giá, báo cáo công tác an toàn, an ninh thông tin của các cơ quan để xác lập

bảng xếp hạng an toàn, an ninh thông tin; đề xuất Ủy ban nhân dân tỉnh xem xét, khen thưởng các tập thể, cá nhân có thành tích xuất sắc trong việc bảo đảm an toàn, an ninh thông tin theo quy định hiện hành.

2. Các tổ chức, các nhân vi phạm Quy chế này tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật hành chính hoặc bị truy cứu trách nhiệm hình sự. Nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật hiện hành.

Điều 12. Trách nhiệm thi hành

1. Giám đốc các sở, ban, ngành; Chủ tịch Ủy ban nhân dân các huyện, thành phố và thủ trưởng các đơn vị thuộc tỉnh chịu trách nhiệm tổ chức triển khai, thực hiện Quy chế này tại cơ quan.

2. Trong quá trình thực hiện, nếu có những vấn đề mới phát sinh hoặc cần sửa đổi, bổ sung các cơ quan kịp thời có văn bản gửi Sở Thông tin và Truyền thông để tổng hợp, báo cáo Ủy ban nhân dân tỉnh xem xét, quyết định./.

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Phan Văn Đa