ỦY BAN NHÂN DÂN TỈNH BÌNH PHƯỚC	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số: 30 /2016/QĐ-UBND	*Đồng Xoài, ngày 01 tháng 7 năm 2016*

QUYẾT ĐỊNH
Ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin trên địa bàn tỉnh Bình Phước

ỦY BAN NHÂN DÂN TỈNH

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

Căn cứ Luật ban hành văn bản quy phạm pháp luật của HĐND, UBND ngày 03/12/2004;

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

Căn cứ Luật Viễn thông ngày 23/11/2009;

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

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 Nghị định số 90/2008/NĐ-CP ngày 13/8/2008 của Chính phủ về chống thư rác;

Căn cứ Nghị định số 77/2012/NĐ-CP ngày 05/10/2012 của Chính phủ về sửa đổi, bổ sung một số điều của Nghị định số 90/2008/NĐ-CP ngày 13/8/2008 của Chính phủ về chống thư rác;

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

Căn cứ Thông tư số 23/2011/TT-BTTTT ngày 11/8/2011 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về việc quản lý, vận hành, sử dụng và bảo đảm an toàn thông tin trên Mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước;

Căn cứ Thông tư số 27/2011/TT-BTTTT ngày 04/10/2011 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối các hoạt động ứng cứu sự cố mạng Internet Việt Nam;

Thực hiện Quyết định số 63/QĐ-TTg ngày 13/01/2010 của Thủ tướng Chính phủ về việc phê duyệt Quy hoạch phát triển an toàn thông tin số quốc gia đến năm 2020;

Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Tờ trình số

11/TTr-STTTT ngày 28/3/2016,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin trên địa bàn tỉnh Bình Phước.

Điều 2. Các ông (bà): Chánh Văn phòng UBND tỉnh; Giám đốc Sở Thông tin và Truyền thông; Thủ trưởng các cơ quan, đơn vị có liên quan; Chủ tịch UBND các huyện, thị xã; Chủ tịch UBND các xã, phường, thị trấn và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này.

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

Nơi nhận:
- Văn phòng Chính phủ;
- Bộ Thông tin và Truyền thông;
- Cục KTVBQPPL - Bộ Tư pháp;
- TTTU, TT.HĐND tỉnh,
- BTT UBMTTQVN tỉnh;
- CT, các PCT UBND tỉnh;
- Như Điều 2;
- Sở Tư pháp;
- LĐVP, Phòng: VX;
- Trung tâm TH-CB;
- Lưu: VT, (TD1-16).

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

Huỳnh Thị Hằng

ỦY BAN NHÂN DÂN TỈNH BÌNH PHƯỚC	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc

QUY CHẾ
Đảm bảo an toàn thông tin trong hoạt động ứng dụng CNTT trên địa bàn tỉnh Bình Phước

(Ban hành kèm theo Quyết định số ..10../2016/QĐ-UBND ngày .01.. tháng..1... năm 2016 của Ủy ban nhân dân tỉnh)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về công tác đảm bảo an toàn thông tin trong hoạt động ứng dụng CNTT trong cơ quan Nhà nước, cơ quan đoàn thể, tổ chức chính trị, tổ chức chính trị xã hội, các doanh nghiệp nhà nước, doanh nghiệp viễn thông, công nghệ thông tin (CNTT) trên địa bàn tỉnh Bình Phước.

Điều 2. Đối tượng áp dụng

1. Quy chế này áp dụng đối với các cơ quan, đơn vị trên địa bàn tỉnh, bao gồm:

a) Ủy ban nhân dân tỉnh và các cơ quan chuyên môn trực thuộc; các cơ quan thuộc ngành dọc trên địa bàn tỉnh.

b) Ủy ban nhân dân các huyện, thị xã và các phòng, ban chuyên môn trực thuộc;

c) Tổ chức chính trị, tổ chức chính trị xã hội, cơ quan đoàn thể;

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

e) Các đơn vị sự nghiệp công lập; các doanh nghiệp nhà nước trên địa bàn tỉnh; các tổ chức, đoàn thể; các doanh nghiệp viễn thông, CNTT.

f) 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.

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

Điều 3. Giải thích từ ngữ

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

1. An toàn thông tin: bao gồm các hoạt động quản lý, nghiệp vụ và kỹ thuật đối với hệ thống thông tin nhằm bảo vệ, khôi phục các hệ thống, các dịch vụ và nội dung thông tin đối với nguy cơ tự nhiên hoặc do con người gây ra. Việc

bảo vệ thông tin, tài sản và con người trong hệ thống thông tin nhằm bảo đảm cho các hệ thống thực hiện đúng chức năng, phục vụ đúng đối tượng một cách sẵn sàng, chính xác và tin cậy. An toàn thông tin bao hàm các nội dung bảo vệ và bảo mật thông tin, an toàn dữ liệu, an toàn máy tính và an toàn mạng.

2. An ninh thông tin là việc bảo đảm thông tin trên mạng không gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

3. Hệ thống thông tin là tập hợp các thiết bị viễn thông, CNTT bao gồm phần cứng, phần mềm và cơ sở dữ liệu phục vụ cho hoạt động lưu trữ, xử lý, truyền đưa, chia sẻ, trao đổi, cung cấp và sử dụng thông tin.

4. Phần mềm độc hại: là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

5. Thông tin số: là thông tin được tạo lập bằng phương pháp dùng tín hiệu số.

6. Máy chủ (server): là máy tính được kết nối với hệ thống mạng LAN, WAN hoặc mạng internet, có năng lực xử lý cao, trên đó cài đặt các phần mềm để phục vụ cho các máy tính khác truy cập, yêu cầu cung cấp các dịch vụ và tài nguyên.

Điều 4. Nguyên tắc bảo đảm an toàn thông tin

1. Tổ chức, cá nhân tham gia cung cấp và sử dụng dịch vụ Internet và thông tin trên mạng có trách nhiệm bảo đảm an toàn thông tin và an ninh thông tin trong phạm vi hệ thống thông tin của mình; phối hợp với cơ quan quản lý nhà nước có thẩm quyền và tổ chức, cá nhân khác trong việc bảo đảm an toàn thông tin và an ninh thông tin trên mạng.

2. Hoạt động bảo đảm an toàn thông tin và an ninh thông tin trên mạng phải được thực hiện thường xuyên, liên tục và hiệu quả trên cơ sở bảo đảm tuân thủ tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin và quy định pháp luật về chất lượng dịch vụ viễn thông, Internet.

3. Việc bảo đảm an toàn thông tin là yêu cầu bắt buộc trong quá trình thiết kế, xây dựng, vận hành, nâng cấp và hủy bỏ các hạ tầng kỹ thuật của cơ quan nhà nước.

4. Thông tin số thuộc quy định danh mục bí mật nhà nước của các cơ quan nhà nước phải được phân loại, lưu trữ, bảo vệ trên cơ sở quy định của pháp luật về bảo vệ bí mật nhà nước.

5. Cơ quan nhà nước phải xây dựng nội quy bảo đảm an toàn hệ thống thông tin trong hoạt động của đối tượng áp dụng quy định tại Điều 2; có cán bộ phụ trách quản lý an toàn thông tin; áp dụng, hướng dẫn và kiểm tra định kỳ việc thực hiện các biện pháp bảo đảm cho hệ thống thông tin trên mạng đáp ứng các tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin.

6. Áp dụng quy trình bảo đảm an toàn dữ liệu bao gồm:

a) Lưu trữ dự phòng;

b) Sử dụng mật mã để bảo đảm an toàn và bảo mật dữ liệu trong lưu trữ và giao dịch theo quy định của Nhà nước về mật mã;

c) Quản lý chặt chẽ việc di chuyển các trang thiết bị CNTT lưu trữ các thông tin thuộc danh mục bí mật nhà nước;

d) Giám sát các khâu tạo lập, xử lý và hủy bỏ dữ liệu;

đ) Các quy trình bảo đảm an toàn dữ liệu khác.

7. Áp dụng quy trình quản lý an toàn hạ tầng kỹ thuật bao gồm:

a) Các giải pháp bảo vệ nhằm ngăn chặn và phát hiện sớm việc truy cập trái phép vào mạng máy tính hay thiết bị lưu trữ dữ liệu;

b) Áp dụng các công nghệ xác thực, cơ chế quản lý quyền truy cập và cơ chế ghi biên bản hoạt động của hệ thống để quản lý và kiểm tra việc truy cập mạng;

c) Kiểm soát chặt chẽ việc cài đặt các phần mềm mới lên máy chủ và máy trạm;

d) Theo dõi thường xuyên tình trạng lây nhiễm và thực hiện loại bỏ phần mềm độc hại khỏi hệ thống;

đ) Các quy trình quản lý an toàn hạ tầng kỹ thuật khác.

8. Điều kiện bảo đảm thực hiện nhiệm vụ an toàn thông tin:

a) Cán bộ, công chức, viên chức phải nắm vững các quy định của pháp luật và nội quy của cơ quan về an toàn thông tin;

b) Cán bộ kỹ thuật về an toàn thông tin phải được tuyển chọn, đào tạo, huấn luyện, thường xuyên bồi dưỡng nghiệp vụ phù hợp với nhiệm vụ được giao và được tạo điều kiện làm việc phù hợp;

c) Cơ quan nhà nước ưu tiên sử dụng lực lượng kỹ thuật về an toàn thông tin của mình; khi cần thiết có thể sử dụng dịch vụ của các tổ chức bảo đảm an toàn thông tin đủ năng lực được Nhà nước công nhận;

d) Hạ tầng kỹ thuật phải được định kỳ kiểm tra, đánh giá hoặc kiểm định về mặt an toàn thông tin phù hợp các tiêu chuẩn, quy chuẩn kỹ thuật quy định.

Điều 5. Các hành vi nghiêm cấm

1. Lưu trữ trên máy tính có kết nối mạng các văn bản, tài liệu, số liệu thuộc bí mật nhà nước hoặc những thông tin, tài liệu mật khác do pháp luật quy định và chỉ được phép cung cấp, chia sẻ cho bên thứ ba có thẩm quyền trong những trường hợp nhất định theo quy định của pháp luật.

2. Các hành vi phá hoại, sử dụng các phương tiện kỹ thuật gây nguy hại cho hệ thống thông tin, làm rối loạn, tê liệt một phần hoặc toàn bộ hệ thống thông tin của các cơ quan nhà nước.

3. Truy nhập khai thác, sử dụng, phát tán, thay đổi, phá hủy các thông tin số thuộc sở hữu của các cá nhân, tổ chức khác khi chưa được phép của chủ sở hữu.

4. Tạo ra, cài đặt, phát tán vi rút, mã độc vào máy tính, mạng LAN, mạng truyền số liệu chuyên dùng của các cơ quan nhà nước.

5. Ngăn chặn việc truy nhập đến thông tin của tổ chức, cá nhân khác trên môi trường mạng, trừ trường hợp pháp luật cho phép.

6. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã của tổ chức và cá nhân khác trên môi trường mạng.

7. Tổ chức, cá nhân, cán bộ công chức, viên chức che giấu tên của mình hoặc giả mạo tên của tổ chức, cá nhân khác khi gửi thông tin trên môi trường mạng LAN, mạng truyền số liệu chuyên dùng của các cơ quan nhà nước.

8. Lợi dụng chức vụ, quyền hạn trong quản lý về an ninh thông tin để gây cản trở hoạt động hợp pháp của các chủ thể tham gia hệ thống mạng LAN, mạng truyền số liệu chuyên dùng của các cơ quan nhà nước, dịch vụ hành chính công; xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức và công dân.

9. Nghiêm cấm tiết lộ tài khoản truy nhập, đấu nối, truy nhập trái phép vào các hệ thống thông tin dùng chung của tỉnh.

10. Các hành vi bị nghiêm cấm tại Điều 12 Luật CNTT năm 2006; các hành vi khác do các cơ quan quản lý nhà nước quy định nội bộ và pháp luật cấm.

Chương II
NỘI DUNG ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 6. Bảo đảm an toàn mạng và hạ tầng kỹ thuật

1. Đảm bảo an toàn cho mạng nội bộ:

a) Mạng nội bộ các cơ quan, đơn vị khi kết nối với hệ thống bên ngoài phải sử dụng tường lửa để ngăn chặn và phát hiện các xâm nhập trái phép vào hệ thống nội bộ như thiết bị tường lửa chuyên dụng hoặc phần mềm tường lửa.

b) Hệ thống mạng không dây (Wifi) phải được thiết lập mật khẩu truy nhập đủ mạnh và thường xuyên thay đổi mật khẩu nhằm tăng cường công tác bảo mật.

c) Xây dựng và áp dụng các biện pháp bảo vệ, giám sát, ghi nhật ký hoạt động hệ thống thông tin nhằm phòng ngừa, ngăn chặn và phát hiện sớm các truy nhập trái phép.

d) Thiết lập, cấu hình đầy đủ các tính năng của thiết bị an toàn mạng. Thường xuyên kiểm tra nhằm kịp thời phát hiện những dấu hiệu bất thường gây mất an toàn cho hệ thống mạng nội bộ của cơ quan, đơn vị.

đ) Kiểm soát chặt chẽ việc cài đặt các phần mềm lên các máy chủ và máy trạm, đảm bảo tuân thủ quy định quản lý an toàn, an ninh thông tin của cơ quan, đơn vị và các quy định khác có liên quan.

e) Cài đặt phần mềm phòng, chống virus, mã độc cho tất cả các máy tính trong mạng nội bộ của cơ quan, đơn vị, thiết lập chế độ cập nhật hàng ngày cho phần mềm này.

g) Kích hoạt và thiết lập chế độ tự động cập nhật bản vá lỗ hổng bảo mật cho các phần mềm trên mỗi máy tính cá nhân; đặt mật khẩu đăng nhập, chế độ bảo vệ màn hình cho máy tính cá nhân nhằm hạn chế các nguy cơ xâm nhập trái phép.

h) Không cài đặt phần mềm không rõ nguồn gốc, xuất xứ; không truy nhập những trang web có nội dung không lành mạnh, không mở những thư điện tử không rõ địa chỉ người gửi.

i) Cá nhân sử dụng hệ thống thông tin không được tự ý gỡ bỏ các phần mềm phòng chống mã độc trên máy tính khi chưa có sự đồng ý của người có thẩm quyền theo quy định của cơ quan, đơn vị.

k) Tất cả các tập tin, thư mục phải được quét mã độc trước khi sao chép, sử dụng.

2. An toàn cho máy chủ:

a) Thiết lập chế độ tự động cập nhật bản vá lỗ hổng bảo mật cho phần mềm hệ điều hành, các phần mềm ứng dụng và hệ quản trị cơ sở dữ liệu được cài đặt trên máy chủ; đóng tất cả các cổng (Port) dịch vụ khi không sử dụng; thiết lập chính sách ghi nhật ký hoạt động hệ thống thông tin (Log file) nhằm phòng ngừa, ngăn chặn và phát hiện sớm các truy nhập trái phép.

b) Khi cần kết nối từ xa, nhất là từ Internet vào máy chủ để quản trị, phải sử dụng phương thức kết nối có mã hóa.

c) Máy chủ chỉ được dùng để cài đặt các phần mềm, dịch vụ dùng chung của cơ quan, đơn vị; không cài đặt phần mềm không rõ nguồn gốc, phần mềm không có nhu cầu sử dụng trên máy chủ.

d) Tất cả các máy chủ phải được trang bị phần mềm phòng chống mã độc, các phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc khi sao chép, mở các tập tin.

đ) Đối với các máy chủ cài đặt các hệ thống thông tin dùng chung; các máy chủ dùng cài đặt, lưu trữ, xử lý thông tin phục vụ cho nhiều cơ quan, đơn vị phải bố trí phòng máy chủ độc lập, phân công bộ phận chuyên trách hoặc cán bộ chuyên trách CNTT trực tiếp quản lý, áp dụng các biện pháp kiểm soát ra vào thích hợp. Phòng máy chủ nên được lắp đặt hệ thống camera giám sát. Quá trình vào, ra phòng máy chủ phải được ghi nhận vào nhật ký quản lý phòng máy chủ.

3. An toàn khi sử dụng các thiết bị lưu trữ ngoài:

a) Việc sử dụng các thiết bị lưu trữ ngoài như ổ cứng di động, thiết bị lưu trữ USB, thẻ nhớ... phải quét virus trước khi đọc hoặc sao chép dữ liệu.

b) Hạn chế tối đa việc sử dụng các thiết bị lưu trữ ngoài để sao chép, di chuyển dữ liệu.

Điều 7. Bảo đảm an toàn trong phát triển hệ thống thông tin, trao đổi thông tin trên môi trường mạng

1. Khi xây dựng mới hệ thống thông tin hoặc nâng cấp, mở rộng hệ thống thông tin hiện tại, phải đưa ra các yêu cầu về an toàn, bảo mật cho hệ thống.

2. Khuyến khích áp dụng công nghệ mã hóa, chữ ký số khi chia sẻ, lưu trữ, trao đổi thông tin trên môi trường mạng.

3. Cán bộ, công chức, viên chức chỉ sử dụng thư điện tử công vụ và các công cụ trao đổi thông tin do các cơ quan nhà nước hoặc tổ chức có thẩm quyền cung cấp để trao đổi thông tin, tài liệu trong hoạt động công vụ. Không sử dụng các phương tiện trao đổi thông tin công cộng trên Internet cho mục đích này.

Điều 8. Quản lý truy cập các hệ thống thông tin

1. Giới hạn số lần đăng nhập sai liên tiếp vào hệ thống. Thiết lập chế độ tự động khóa tạm thời tài khoản nếu liên tục đăng nhập sai vượt quá số lần quy định.

2. Hủy bỏ, thu hồi quyền truy cập vào hệ thống thông tin, thu hồi lại tất cả các tài sản liên quan tới hệ thống thông tin của cơ quan (máy vi tính, tài khoản,...) khi cán bộ, công chức, viên chức và người lao động nghỉ hưu, chuyển công tác hoặc nghỉ việc.

3. Mật khẩu truy cập vào các hệ thống thông tin phải có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự số và ký tự đặc biệt như !, @, #, $, %,...).

4. Tất cả máy trạm, máy chủ phải được đặt mật khẩu truy nhập và thiết lập chế độ tự động bảo vệ màn hình sau 10 phút không sử dụng.

Điều 9. Sao lưu dữ liệu

1. Ban hành kế hoạch và thực hiện sao lưu, phục hồi cho các phần mềm, dữ liệu cần thiết.

2. 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.

3. Dữ liệu sao lưu phải được lưu trữ an toàn và được kiểm tra thường xuyên bảo đảm khả năng sẵn sàng cho việc sử dụng khi cần. Kiểm tra khả năng phục hồi hệ thống từ dữ liệu sao lưu tối thiểu 6 tháng một lần.

Điều 10. Quy định sử dụng các hệ thống thông tin dùng chung của tỉnh

1. Tài khoản truy nhập các hệ thống thông tin dùng chung của tỉnh phải đổi mật khẩu mặc định ngay sau khi được các cơ quan quản lý hệ thống dùng

chung cấp. Mật khẩu phải được thay đổi định kỳ và được đặt theo quy định tại khoản 3, Điều 8 Quy chế này.

2. Không đặt chế độ tự động lưu trữ mật khẩu trong các trình duyệt trong mọi trường hợp sử dụng.

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 11. Trách nhiệm của cán bộ, công chức, viên chức, người lao động

1. Nghiêm chỉnh chấp hành các quy chế nội bộ, quy trình về an toàn, an ninh thông tin của cơ quan, đơn vị cũng như quy định khác của pháp luật, nâng cao ý thức cảnh giác và trách nhiệm bảo đảm an toàn, an ninh thông tin tại đơn vị.

2. Cán bộ, công chức, viên chức, người lao động phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp các thiết bị trên máy tính; không được vào các trang web không rõ về nội dung; không sử dụng thiết bị lưu trữ ngoài không rõ nguồn gốc; không tải và cài đặt các phần mềm không rõ nguồn gốc, không liên quan đến công việc chuyên môn; không nhấp chuột vào các đường dẫn lạ không rõ về nội dung.

3. Trách nhiệm của cán bộ công chức, viên chức chuyên trách hoặc cán bộ công chức, viên chức được giao phụ trách CNTT trong các cơ quan, đơn vị chịu trách nhiệm triển khai các biện pháp quản lý, vận hành, quản lý kỹ thuật, tham mưu xây dựng quy định về đảm bảo an toàn cho hệ thống thông tin của cơ quan, đơn vị theo quy chế này. Phối hợp với với các cá nhân, các cơ quan, đơn vị có liên quan trong việc kiểm tra, phát hiện và khắc phục sự cố mất an toàn thông tin

4. Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin phải báo cáo ngay với cấp trên và bộ phận chuyên trách CNTT của đơn vị để kịp thời ngăn chặn và xử lý.

Điều 12. 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 trước Ủy ban nhân dân tỉnh trong công tác đảm bảo an toàn, an ninh thông tin của đơn vị mình.

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

3. Để dữ liệu của các cơ quan, đơn vị được bảo mật thì các cơ quan, đơn vị phải quy định các dữ liệu cần thiết để bảo mật, tránh rò rỉ, mất thông tin. Quy định trách nhiệm bảo mật thông tin được giao cho người nào quản lý thì người đó có trách nhiệm bảo mật, lưu trữ.

4. Phân công cán bộ công chức, viên chức có chuyên môn phụ trách an toàn thông tin của cơ quan; tạo điều kiện để các cán bộ công chức, viên chức phụ trách an toàn thông tin được học tập, nâng cao trình độ về an toàn, an ninh thông tin.

5. Khi có sự cố hoặc nguy cơ mất an toàn 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 ninh thông tin của đơn vị và lập biên bản báo cáo bằng văn bản cho cơ quan cấp trên quản lý trực tiếp và Sở Thông tin và Truyền thông để cùng phối hợp xử lý.

6. 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 một cách kịp thời, nhanh chóng và đạt hiệu quả.

7. Khi triển khai đầu tư ứng dụng CNTT phải có phương án đảm bảo an toàn thông tin từ khâu thiết kế và phải tự chịu trách nhiệm đảm bảo an toàn thông tin cho hệ thống CNTT và các hệ thống thông tin của các cơ quan, đơn vị mình.

8. Trang bị đầy đủ các kiến thức bảo mật cơ bản cho cán bộ, công chức, viên chức về an toàn thông tin trước khi cho phép truy nhập và sử dụng hệ thống thông tin.

9. Phối hợp chặt chẽ với Công an tỉnh trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn, an ninh thông tin.

10. Định kỳ hằng năm trước ngày 30/10 hoặc đột xuất báo cáo về tình hình an toàn, an ninh thông tin của cơ quan gửi về Sở Thông tin và Truyền thông để tổng hợp.

Điều 13. Trách nhiệm của Sở Thông tin và Truyền thông

1. Tham mưu UBND tỉnh về công tác đảm bảo an toàn, an ninh thông tin trên địa bàn tỉnh.

2. Hằng năm xây dựng kế hoạch triển khai công tác đảm bảo an toàn thông tin phục vụ cho việc vận hành các hệ thống thông tin được UBND tỉnh giao quản lý.

3. Định kỳ hàng năm, tiến hành kiểm tra đột xuất các cơ quan, đơn vị có dấu hiệu vi phạm an toàn thông tin.

4. Chủ trì, phối hợp với Công an tỉnh và các cơ quan, đơn vị có liên quan để tham mưu thành lập Đoàn kiểm tra; xây dựng kế hoạch kiểm tra và tiến hành công tác kiểm tra an toàn thông tin tại tất cả các cơ quan, đơn vị.

5. Chủ trì hoạt động thanh tra và xử lý các hành vi vi phạm về an toàn thông tin và phát tán tin nhắn rác trên địa bàn tỉnh. Phối hợp với Công an tỉnh tiến hành xử phạt các hành vi vi phạm an toàn thông tin gây thiệt hại cho hệ thống tin thuộc các cơ quan, đơn vị nhà nước thuộc tỉnh.

6. Hằng năm xây dựng và triển khai các chương trình đào tạo chuyên sâu về an toàn, an ninh thông tin cho lực lượng đảm bảo an toàn, an ninh thông tin của các cơ quan, đơn vị.

7. Tổ chức các hội nghị, hội thảo chuyên đề và tuyên truyền về an toàn, an ninh thông tin trong công tác quản lý nhà nước trên địa bàn tỉnh.

8. Tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin.

9. Tùy theo tính chất mức độ sự cố mất an toàn thông tin, phối hợp Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) và các cơ quan có liên quan hướng dẫn xử lý, ứng cứu các sự cố mất an toàn, an ninh thông tin.

10. Hướng dẫn, giám sát các cơ quan, đơn vị trên địa bàn tỉnh xây dựng quy chế nội bộ và thực hiện việc đảm bảo an toàn, an ninh cho hệ thống thông tin theo quy định của Nhà nước.

11. Tổng hợp và báo cáo về tình hình an toàn, an ninh thông tin theo định kỳ hoặc đột xuất báo cáo UBND tỉnh, Bộ Thông tin và Truyền thông và các cơ quan, đơn vị có liên quan .

Điều 14. Trách nhiệm của Công an tỉnh

1. Chủ trì, phối hợp với Sở Thông tin và Truyền thông, các cơ quan, đơn vị có liên quan xây dựng kế hoạch và chịu trách nhiệm kiểm soát, phòng ngừa, đấu tranh, ngăn chặn các loại tội phạm lợi dụng hệ thống thông tin 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 xâm phạm 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 địa bàn tỉnh.

Điều 15. Trách nhiệm Sở Tài chính

Tham mưu UBND tỉnh bố trí kinh phí để thực hiện các nhiệm vụ bảo đảm an toàn thông tin, an ninh thông tin của tỉnh, nhất là trong trường hợp phát sinh sự cố khẩn cấp.

Điều 16. Trách nhiệm của tổ chức, doanh nghiệp, cá nhân đối với việc bảo đảm an toàn, an ninh thông tin

1. Các tổ chức, doanh nghiệp cung cấp dịch vụ hạ tầng mạng, Internet, CNTT phải thiết lập đầu mối liên lạc để phối hợp, tuân thủ việc điều phối của cơ quan chức năng và tham gia vào công tác ứng cứu, khắc phục sự cố cho hệ thống thông tin của tỉnh.

2. Tổ chức, cá nhân tham gia cung cấp thông tin và sử dụng dịch vụ trên mạng có trách nhiệm bảo đảm an toàn, an ninh thông tin trong phạm vi hệ thống thông tin của mình; phối hợp với cơ quan quản lý nhà nước có thẩm quyền và tổ chức, cá nhân khác trong việc bảo đảm an toàn, an ninh thông tin trên mạng.

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

4. Thực hiện các nghĩa vụ, trách nhiệm khác theo các quy định của pháp luật.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 17. Khen thưởng và xử lý vi phạm

1. Các cơ quan, đơn vị và cá nhân có thành tích xuất sắc trong công tác đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin trên địa bàn tỉnh sẽ được xem xét khen thưởng theo quy định.

2. Các cơ quan, đơn vị và cá nhân có hành vi vi phạm Quy chế này tùy theo tính chất, mức độ vi phạm sẽ bị xử lý theo quy định của pháp luật.

Điều 18. Điều khoản thi hành

1. Thủ trưởng các cơ quan, đơn vị nhà nước trên địa bàn tỉnh Bình Phước chịu trách nhiệm tổ chức triển khai thực hiện Quy chế tại đơn vị mình.

2. Đối với các nội dung khác liên quan đến công tác đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin không được quy định trong Quy chế này thì thực hiện theo quy định về đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin đã được quy định trong các văn bản quy phạm pháp luật của Trung ương.

3. Trong quá trình thực hiện, nếu có những vấn đề cần sửa đổi, bổ sung, đề nghị các đơn vị gửi văn bản về Sở Thông tin và Truyền thông để tổng hợp, báo cáo UBND tỉnh xem xét giải quyết./.

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

Huỳnh Thị Hằng