ỦY BAN NHÂN DÂN TỈNH TIỀN GIANG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 42/2015/QĐ-UBND	*Tiền Giang, ngày 21 tháng 12 năm 2015*

QUYẾT ĐỊNH
Ban hành Quy chế bảo đảm an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Tiền Giang

ỦY BAN NHÂN DÂN TỈNH TIỀN GIANG

Căn cứ Luật Tổ chức Hội đồng nhân dân và Uỷ ban nhân dân ngày 26 tháng 11 năm 2003;

Căn cứ Luật Ban hành văn bản quy phạm pháp luật của Hội đồng nhân dân và Ủy ban nhân dân ngày 03 tháng 12 năm 2004;

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

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

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ về Ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

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

Căn cứ Thông tư số 23/2011/TT-BTTTT ngày 11 tháng 8 năm 2011 của 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;

Theo 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 trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Tiền Giang.

Điều 2. Quyết định này có hiệu lực thi hành sau 10 ngày, kể từ ngày ký. Giám đốc Sở Thông tin và Truyền thông có trách nhiệm phối hợp với Thủ trưởng các sở, ngành liên quan triển khai thực hiện Quyết định này.

Điều 3. Chánh Văn phòng Ủy ban nhân dân tỉnh, Giám đốc Sở Thông tin và Truyền thông; Thủ trưởng các sở, ban, ngành tỉnh; Chủ tịch Ủy 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;
- Văn phòng Chính phủ;
- Bộ Thông tin và Truyền thông;
- Bộ Tư pháp (Cục Kiểm tra VB);
- TT.TU, TT.HĐND tỉnh;
- TT.UBMTTQ tỉnh;
- CT, các PCTUBND tỉnh;
- VPUB: CVP và các PCVP, các Phòng NC, Ban TCD;
- Công ty Điện lực TG;
- Cổng TTĐT, Công báo tỉnh;
- Lưu: VT, P.KTN (Tâm). 15

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

ỦY BAN NHÂN DÂN TỈNH TIỀN GIANG

Trần Thanh Đức

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

QUY CHẾ

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

(Ban hành kèm theo Quyết định số: 42/2015/QĐ-UBND ngày 21/12/2015 của Ủy ban nhân dân tỉnh Tiền Giang)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về nội dung bảo đảm an toàn thông tin, trách nhiệm của các cơ quan nhà nước, tổ chức, cá nhân có liên quan trong việc đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin (CNTT) của các cơ quan nhà nước trên địa bàn tỉnh Tiền Giang.

Điều 2. Đối tượng áp dụng

1. Các cơ quan nhà nước (CQNN) và cán bộ, công chức, viên chức và người lao động trong các CQNN trên địa bàn tỉnh Tiền Giang.

2. 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.

3. Khuyến khích các cơ quan Đảng, đoàn thể, tổ chức chính trị - xã hội áp dụng quy chế này trong hoạt động ứng dụng CNTT.

Điều 3. Giải thích từ ngữ

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

1. Hạ tầng kỹ thuật: Là tập hợp thiết bị tính toán (máy chủ, máy trạm), thiết bị ngoại vi, thiết bị kết nối mạng, thiết bị lưu trữ thông tin, thiết bị phụ trợ, mạng nội bộ, mạng diện rộng.

2. An toàn thông tin: Là sự bảo vệ thông tin và các hệ thống thông tin tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

3. 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.

4. Mạng nội bộ (LAN - Local Area Networks): Mạng máy tính được thiết lập bằng cách kết nối các máy tính trong cùng một cơ quan, đơn vị cùng một trụ sở, nhằm chia sẻ tài nguyên, thiết bị dùng chung (như tập tin, máy in, máy quét...).

5. Mạng diện rộng (WAN) của tỉnh: Mạng máy tính được thiết lập bằng cách kết nối giữa Trung tâm Tích hợp dữ liệu tỉnh Tiền Giang với các mạng LAN của các cơ quan, đơn vị thông qua mạng truyền số liệu chuyên dùng của các cơ quan nhà nước.

6. Mạng truyền số liệu chuyên dùng của các cơ quan nhà nước: Mạng truyền dẫn tốc độ cao, sử dụng phương thức chuyển mạch nhãn đa giao thức trên nền giao thức liên mạng (IP/MPLS) sử dụng riêng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước do Tập đoàn Bưu chính Viễn thông Việt Nam xây dựng, vận hành.

7. Mạng Internet: Mạng máy tính toàn cầu, kết nối tới rất nhiều máy tính và mạng máy tính con trên toàn thế giới.

8. Hệ thống thông tin: Tập hợp các thiết bị viễn thông, công nghệ thông tin 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.

9. Ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước: Theo khoản 1 Điều 3 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.

10. Cơ sở dữ liệu (database): Là một hệ thống các thông tin có cấu trúc hoặc không cấu trúc được lưu trữ trên các thiết bị lưu trữ thứ cấp (băng từ, đĩa từ...) nhằm thỏa mãn yêu cầu khai thác thông tin đồng thời của nhiều người sử dụng hay nhiều chương trình, phần mềm ứng dụng với nhiều mục đích khác nhau.

11. Máy chủ (Server): 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 hoặc cơ sở dữ liệu.

Điều 4. Nguyên tắc chung về bảo đảm an toàn thông tin

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

2. Các cơ quan, tổ chức, cá nhân và CBCCVC chịu trách nhiệm trước pháp luật về nội dung thông tin đã chuyển đi trên mạng nội bộ (LAN), mạng truyền số liệu chuyên dùng của các cơ quan nhà nước và mạng Internet.

3. Bảo đảm an toàn hệ thống thông tin trong hoạt động của cơ quan nhà nước.

4. Tuân thủ các nguyên tắc, các tiêu chuẩn, quy chuẩn kỹ thuật về bảo mật, an toàn thông tin.

5. Kết hợp nhiều biện pháp bảo đảm an toàn thông tin trên môi trường mạng, nhằm kịp thời phát hiện và ngăn chặn các nguy cơ mất an toàn, an ninh thông tin.

Điều 5. Các hành vi nghiêm cấm

1. Lưu trữ, dự thảo 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.

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 cập, khai thác, sử dụng, phát tán, thay đổi, phá hủy các thông tin 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 máy tính vào hệ thống thông tin 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. Giải mã, trộm cắp, sử dụng mật khẩu khi chưa được sự đồng ý của các tổ chức, cá nhân chủ quản hệ thống thông tin.

7. Tổ chức, cá nhân, CBCCVC 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, tham gia dịch vụ hành chính công trên Internet; xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức và công dân.

9. Các hành vi bị nghiêm cấm tại Điều 12 Luật Công nghệ thông tin.

Chương II
NỘI DUNG BẢO ĐẢM 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 cập 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 cập 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 cập những trang web có nội dung không lành mạnh, không mở những thư điện tử không rõ địa chỉ người gửi;

i) Cán bộ, công chức, viên chức và người lao động không được tự ý gỡ bỏ các phần mềm phòng chống mã độc trên máy tính trạm khi chưa có sự đồng ý của người có thẩm quyền theo quy định của cơ quan; Tất cả các tập tin, thư mục phải được quét mã độc trước khi sao chép, sử dụng;

k) Hạn chế sử dụng chức năng chia sẻ (Sharing) thư mục, tránh việc chia sẻ toàn bộ ổ cứng, yêu cầu phải sử dụng mật khẩu khi truy cập thư mục chia sẻ và thực hiện thu hồi chức năng này sau khi đã sử dụng xong.

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 cập 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 phải đảm bảo các điều kiện cho những thiết bị đặt trong đó hoạt động ổn định, các điều kiện tối thiểu gồm: Nguồn cung cấp điện ổn định, có dự phòng; có bình chữa cháy hoặc hệ thống tự động cảnh báo, chữa cháy khẩn cấp; hệ thống phòng, chống sét; được bố trí ở khu vực có điều kiện an ninh tốt; có máy điều hòa không khí;

e) Khi bảo trì, sửa chữa máy chủ phải ghi lại nhật ký vào sổ theo dõi, cán bộ chuyên trách hoặc phụ trách công nghệ thông tin có trách nhiệm ký xác nhận vào sổ theo dõi ghi lại nhật ký sau mỗi lần bảo trì, sửa chữa.

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) Các thiết bị lưu trữ ngoài chứa 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 không được kết nối vào các máy tính có nối mạng và không được mang ra ngoài cơ quan trừ khi có sự đồng ý của Thủ trưởng đơn vị;

c) 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. 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 chấm dứt lao động hợp đồng.

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).

4. Tất cả máy trạm, máy chủ phải được đặt mật khẩu truy cập và thiết lập chế độ tự động bảo vệ màn hình.

Điều 9. Sao lưu dữ liệu

1. Ban hành và thực hiện quy trình 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. Nghiêm cấm tiết lộ tài khoản truy cập, đấu nối, truy cập trái phép vào các hệ thống thông tin dùng chung của tỉnh.

2. Tài khoản truy cập các hệ thống thông tin dùng chung của tỉnh phải đổi mật khẩu mặc định ngay sau khi được Sở Thông tin và Truyền thông cấp. Mật khẩu phải được thay đổi định kỳ và được đặt theo quy định tại khoản 3, Điều 8 Quy chế này.

3. 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 và người lao động

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

a) Nghiêm chỉnh thi hành quy chế này và các quy định khác của pháp luật về bảo đảm an toàn, an ninh thông tin.

b) Có trách nhiệm quản lý, bảo quản, bảo đảm an toàn cho các thiết bị được giao quản lý, sử dụng.

c) Khi phát hiện sự cố mất an toàn thông tin, an ninh thông tin phải thông báo ngay với cấp trên và cán bộ chuyên trách, phụ trách công nghệ thông tin để kịp thời ngăn chặn, xử lý.

d) Tham gia đầy đủ các chương trình đào tạo, tập huấn về an toàn thông tin, an ninh thông tin do Ủy ban nhân dân tỉnh chỉ đạo tổ chức.

đ) Các thông tin, tài liệu, văn bản có tính mật theo quy định, phải dự thảo, lưu trữ đúng theo quy định về bảo mật và an toàn thông tin.

2. Trách nhiệm của cán bộ chuyên trách, phụ trách công nghệ thông tin:

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

b) Chịu trách nhiệm tham mưu chuyên môn và vận hành đảm bảo an toàn hệ thống thông tin của đơn vị;

c) Hướng dẫn, hỗ trợ người dùng tại đơn vị giải pháp phòng, chống vi rút máy tính. Thực hiện việc đánh giá, báo cáo các rủi ro và mức độ các rủi ro ảnh hưởng đến hoạt động hệ thống thông tin của đơn vị, các giải pháp cơ bản khắc phục các rủi ro;

d) Trực tiếp thiết lập các biện pháp kỹ thuật bảo đảm an toàn cho hạ tầng kỹ thuật, hệ thống thông tin trong cơ quan, đơn vị mình; hướng dẫn cán bộ, công chức, viên chức và người lao động trong cơ quan, đơn vị tuân thủ các biện pháp bảo đảm an toàn thông tin, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin;

đ) Thực hiện việc giám sát, đánh giá, báo cáo thủ trưởng cơ quan các sự cố mất an toàn thông tin và mức độ nghiêm trọng của các sự cố đó;

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

Điều 12. Trách nhiệm của các cơ quan

1. Thủ trưởng 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 bảo đảm an toàn thông tin, an ninh thông tin của đơn vị mình.

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

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

4. Khi bị sự cố an toàn thông tin, cơ quan nhà nước bị sự cố phải thực hiện theo nội dung quy định tại Khoản 1 Điều 42 Nghị định số 64/2007/NĐ-CP.

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 an toàn thông tin, an ninh thông tin kịp thời, nhanh chóng và đạt hiệu quả.

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

7. Định kỳ hằng năm, báo cáo tình hình an toàn thông tin, an ninh thông tin gửi về Sở Thông tin và Truyền thông (trước 26/10 hàng năm).

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

1. Chủ trì, phối hợp với các cơ quan liên quan thành lập đoàn thanh, kiểm tra định kỳ hoặc đột xuất; kịp thời phát hiện và xử lý theo thẩm quyền đối với các hành vi vi phạm an toàn thông tin, an ninh thông tin trên địa bàn tỉnh.

2. Tham mưu Ủy ban nhân dân tỉnh về công tác bảo đảm an toàn thông tin trên địa bàn tỉnh và phối hợp với các đơn vị có liên quan trong việc bảo đảm an toàn cho các hệ thống thông tin của tỉnh.

3. Xây dựng và triển khai các chương trình đào tạo, hội nghị tuyên truyền về an toàn, an ninh thông tin trong công tác quản lý nhà nước trên địa bàn tỉnh.

4. Quản lý vận hành, hướng dẫn kết nối mạng truyền số liệu chuyên dùng của các cơ quan nhà nước trên địa bàn tỉnh.

5. Tùy theo mức độ sự cố, phối hợp Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam và các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố an toàn thông tin trên địa bàn tỉnh.

6. Hướng dẫn cụ thể về nghiệp vụ quản lý vận hành, kỹ thuật đảm bảo an toàn, an ninh thông tin; hỗ trợ các cơ quan, đơn vị giải quyết sự cố.

7. Thường xuyên cập nhật các nguy cơ gây mất an toàn, an ninh thông tin và thông báo cho các cơ quan, đơn vị biết để có biện pháp phòng ngừa, ngăn chặn, xử lý kịp thời.

8. Tổng hợp và báo cáo về tình hình an toàn thông tin, an ninh thông tin theo định kỳ cho Bộ Thông tin và Truyền thông, Ủy ban nhân dân tỉnh và các cơ quan, đơn vị có liên quan.

Điều 14. Trách nhiệm của Công an tỉnh

1. Phối hợp với Sở Thông tin và Truyền thông trong công tác thanh tra, kiểm tra về an toàn thông tin, an ninh thông tin.

2. Tăng cường công tác phòng ngừa, phát hiện, tuyên truyền, phổ biến pháp luật về bảo vệ bí mật nhà nước, về phòng, chống, phát hiện tội phạm trong việc đảm bảo an toàn, an ninh thông tin.

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

Điều 15. Trách nhiệm của Sở Tài chính

Cân đối kinh phí để thực hiện các nhiệm vụ bảo đảm an toàn thông tin, an ninh thông tin của tỉnh theo quy định.

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 giao tiếp.

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, tổ chức, doanh nghiệp và cá nhân có thành tích xuất sắc trong việc đảm bảo an toàn an ninh thông tin trong hoạt động ứng dụng CNTT trên địa bàn tỉnh sẽ được xem xét khen thưởng theo quy định.

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

Điều 18. Điều khoản thi hành

1. Giám đốc Sở Thông tin và Truyền thông có trách nhiệm hướng dẫn, triển khai thực hiện Quy chế này.

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

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

Trần Thanh Đức