ỦY BAN NHÂN DÂN **TỈNH QUẢNG NAM**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 2116/QĐ-UBND	*Quảng Nam, ngày 11 tháng 7 năm 2018*

QUYẾT ĐỊNH

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 Quảng Nam

ỦY BAN NHÂN DÂN TỈNH QUẢNG NAM

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

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

Căn cứ Luật An toàn thông tin mạng ngày 19/11/2015;

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 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Căn cứ Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;

Căn cứ Thông tư số 27/2017/TT-BTTTT ngày 20/10/2017 của Bộ Thông tin và Truyền thông quy định về quản lý, vận hành, kết nối, 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 Sở Thông tin và Truyền thông tại Tờ trình số 174/TTr-STTTT ngày 27/6/2018,

QUYẾT ĐỊNH:

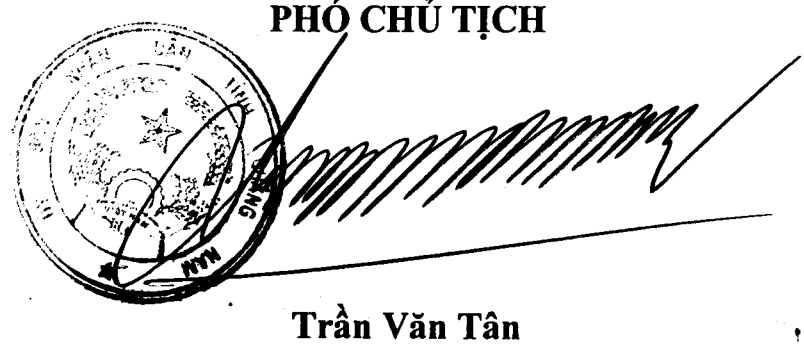
Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng Công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Quảng Nam.

Điều 2. Quyết định này có hiệu lực kể từ ngày ký.

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

Nơi nhận:
- Như điều 3;
- Bộ TTTT;
- TTTU, TT HĐND tỉnh;
- Chủ tịch, các PCT UBND tỉnh;
- CPVP;
- Lưu: VT, KGVX (Hậu)

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



Trần Văn Tân

ỦY BAN NHÂN DÂN TỈNH QUẢNG NAM	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 Quảng Nam

(Ban hành kèm theo Quyết định số 1826/QĐ-UBND ngày 11/7/2018 của UBND tỉnh)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về 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 Quảng Nam.

Điều 2. Đối tượng áp dụng

1. Các Sở, Ban, ngành, UBND các huyện, thị xã, thành phố; các đơn vị sự nghiệp trực thuộc UBND tỉnh; UBND các xã, phường, thị trấn (sau đây gọi tắt là các cơ quan, đơn vị).

2. Các tổ chức, cá nhân, doanh nghiệp có tham gia quản lý, cung cấp, vận hành, khai thác, ứng dụng Công nghệ thông tin trong hoạt động của các cơ quan, đơn vị nêu tại Khoản 1 Điều này.

3. Cán bộ, công chức, viên chức, người lao động đang công tác trong các cơ quan, đơn vị nêu tại Khoản 1 Điều này.

Chương II
NỘI DUNG BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 3. Bảo đảm an toàn hạ tầng ứng dụng công nghệ thông tin

1. Bảo đảm an toàn thông tin chung cho hệ thống thông tin, hệ thống thiết bị mạng, máy chủ, máy tính cá nhân

a) Lãnh đạo cơ quan, đơn vị phải chỉ đạo thực hiện chặt chẽ việc bảo vệ an toàn vật lý cho tất cả hệ thống công nghệ thông tin của cơ quan, đơn vị mình;

b) Hệ thống máy chủ, máy tính cá nhân, hệ thống lưu trữ nội bộ, thiết bị mạng; hệ thống mạng không dây (Wifi) phải được bảo vệ bởi mật khẩu an toàn. Mật khẩu đăng nhập phải có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, gồm ký tự thường, ký tự số và ký tự đặc biệt như !, @, #, $, %,...) và phải định kỳ thay đổi ít nhất 3 tháng/lần.

c) Quản lý đăng nhập hệ thống: Các hệ thống thông tin cần giới hạn số lần đăng nhập, tự động khóa tài khoản khi liên tục đăng nhập sai vượt quá số lần quy định. Tổ chức theo dõi, giám sát tất cả các phương pháp đăng nhập từ xa, nhất là các trường hợp đăng nhập vào hệ thống với mục đích quản trị.

d) Chống phần mềm độc hại: Triển khai các phần mềm chống mã độc trên các máy tính, thiết bị di động trong mạng để phát hiện, loại trừ phần mềm độc hại. Thường xuyên cập nhật các phiên bản mới, các bản vá lỗi của các phần mềm chống virus để bảo đảm chương trình quét virus của cơ quan trên các máy chủ, máy trạm luôn được cập nhật mới nhất; thiết lập chế độ quét thường xuyên ít nhất 1 lần/tuần. Thường xuyên cập nhật bản vá các lỗ hổng bảo mật của hệ điều hành và các phần mềm ứng dụng trên máy tính để hạn chế tối đa rủi ro mất an toàn thông tin mạng.

e) Khi xảy ra sự cố an toàn thông tin mạng thì cơ quan, đơn vị có trách nhiệm thông báo kịp thời cho doanh nghiệp cung cấp dịch vụ hoặc bộ phận chuyên trách ứng cứu sự cố để xây dựng phương án, tổ chức khắc phục. Trong trường hợp không khắc phục được phải thông báo, phối hợp với Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ, khắc phục.

f) Quản lý nhật ký sự kiện (logfile): Hệ thống thông tin cần ghi nhận các sự kiện như: quá trình đăng nhập hệ thống, các thao tác cấu hình hệ thống, quá trình truy xuất hệ thống... Thường xuyên kiểm tra, sao lưu (backup) các nhật ký sự kiện theo từng tháng để theo dõi, xác định những sự kiện đã xảy ra và hạn chế việc tràn nhật ký sự kiện gây ảnh hưởng đến hoạt động của hệ thống.

g) Bảo đảm an toàn cho Cổng/Trang thông tin điện tử: Các đơn vị trong quá trình quản lý, khai thác và cung cấp thông tin trên Cổng/Trang thông tin điện tử của mình phải thường xuyên theo dõi, cập nhật phiên bản vá lỗi nhằm tránh các lỗi đã được công bố; thiết lập và cấu hình hệ thống máy chủ cài đặt Cổng/Trang thông tin điện tử an toàn giảm thiểu khả năng bị tin tặc tấn công. Tổ chức mô hình mạng hợp lý cũng như thiết lập các hệ thống phòng thủ quan trọng như tường lửa (firewall), thiết bị phát hiện/phòng, chống xâm nhập.

h) Xử lý khẩn cấp: Khi phát hiện hệ thống thông tin trên mạng bị tấn công cần thực hiện các bước cơ bản sau:

Bước 1: Ngắt kết nối máy chủ ra khỏi mạng.

Bước 2: Xác minh tình trạng, mức độ, phạm vi sự cố, sau đó phân loại sự cố *(Tấn công thay đổi giao diện, tấn công lừa đảo, tấn công phát tán mã độc, tấn công từ chối dịch vụ...)*

Bước 3: Sao chép nhật ký sự kiện và toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ *(phục vụ cho hoạt động phân tích, điều tra)*. Đối với trường hợp phức tạp không tự xử lý được, thực hiện ngay Bước 4.

Bước 4: Báo cáo kịp thời cho lãnh đạo, các đơn vị có chức năng để kịp thời phối hợp xử lý sự cố.

Bước 5: Khôi phục hệ thống bằng cách chuyển dữ liệu sao lưu mới nhất để hệ thống hoạt động trở lại. Lưu trữ hồ sơ xử lý sự cố.

2. Bảo đảm an toàn với các đơn vị có hệ thống thông tin riêng

a) Các 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 và kiểm soát ra vào thích hợp.

b) 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: được bố trí ở khu vực có điều kiện an ninh tốt; khô ráo, có điều hòa không khí; nguồn cung cấp điện ổn định và có dự phòng; có bình chữa cháy hoặc hệ thống tự động cảnh báo, chữa cháy khẩn cấp; phòng, chống sét; có nội quy hướng dẫn làm việc trong khu vực an toàn bảo mật.

c) Thiết lập cơ chế bảo vệ mạng nội bộ bảo đảm an toàn thông tin khi có kết nối mạng nội bộ với mạng ngoài như: Internet, mạng cơ quan khác; cần sử dụng hệ thống bảo vệ mạng nội bộ như: hệ thống tường lửa, hệ thống chống xâm nhập trái phép...

d) Xây dựng và áp dụng các biện pháp bảo vệ, giám sát, ghi nhật ký hoạt động và quản lý hạ tầng kỹ thuật, hệ thống thông tin nhằm phòng ngừa, ngăn chặn và phát hiện sớm các truy cập trái phép theo điểm c, d, e, f, Khoản 1 Điều này.

e) 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.

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, các loại thẻ nhớ, thiết bị lưu trữ USB,... 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 4. Bảo đảm an toàn dữ liệu, cơ sở dữ liệu và phần mềm ứng dụng công nghệ thông tin

1. Các hệ thống phần mềm ứng dụng, cơ sở dữ liệu phải có cơ chế sao lưu dữ liệu dự phòng, dữ liệu được lưu trữ tại nơi an toàn, đồng thời phải thường xuyên kiểm tra để đảm bảo sẵn sàng phục hồi khi có sự cố an toàn thông tin mạng xảy ra.

2. 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.

3. Quản lý chặt chẽ các thiết bị tin học lưu trữ dữ liệu, nghiêm cấm việc di chuyển, thay đổi vị trí khi chưa được phép của người có thẩm quyền.

4. Quản lý và phân quyền truy cập phần mềm ứng dụng và cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ của người sử dụng.

5. Phần mềm hệ quản trị cơ sở dữ liệu phải được thiết lập cơ chế tự động cập nhật bản vá lỗ hổng bảo mật từ nhà sản xuất.

6. Các thiết bị công nghệ thông tin dùng để soạn thảo, in ấn văn bản, lưu

trữ thông tin bí mật nhà nước trong các cơ quan, đơn vị phải được bố trí riêng, tiến hành ở nơi đảm bảo bí mật, an toàn; không được kết nối vào mạng LAN của đơn vị. Đặc biệt là không được sử dụng máy tính đã nối mạng Internet đánh máy, in, sao tài liệu mật. Trên máy tính này phải thực hiện các chế độ mã hóa, phân quyền và đặt mật khẩu cho người được giao sử dụng để đảm bảo an toàn, bảo mật thông tin.

7. Tuân thủ các quy định khi khai thác, sử dụng các phần mềm dùng chung của tỉnh

a) Khi sử dụng các ứng dụng dùng chung của tỉnh mọi người phải có ý thức tự bảo vệ thông tin cá nhân của mình; nghiêm cấm việc tiết lộ tài khoản đăng nhập của mình cho người không có thẩm quyền hoặc sử dụng trái phép tài khoản của người khác để truy cập trái phép vào hệ thống các phần mềm dùng chung của tỉnh.

b) Người sử dụng phải thay đổi mật khẩu mới sau lần đăng nhập đầu tiên đối với các tài khoản được cung cấp để truy cập các phần mềm, cơ sở dữ liệu dùng chung của tỉnh; không sử dụng chế độ ghi nhớ mật khẩu.

c) Khi khai thác, sử dụng các phần mềm ứng dụng dùng chung của tỉnh tại các điểm truy cập Internet công cộng, tuyệt đối không đặt chế độ ghi nhớ mật khẩu trong các trình duyệt.

d) Đối với cán bộ, công chức, viên chức đã nghỉ việc, chuyển công tác, phải có biện pháp khóa hoặc hủy tài khoản, quyền truy nhập các hệ thống dùng chung, thu hồi các thiết bị công nghệ thông tin liên quan.

Điều 5. Bảo đảm an toàn thông tin Trung tâm tích hợp dữ liệu của tỉnh

1. Xây dựng phương án đảm bảo an toàn thông tin mạng cho Trung tâm tích hợp dữ liệu của tỉnh; bảo đảm an toàn và thuận lợi đối với quá trình quản lý và sử dụng các dịch vụ.

2. Các cơ quan, đơn vị đặt dữ liệu hoặc kết nối vào Trung tâm tích hợp dữ liệu của tỉnh phải tuân thủ các chính sách an toàn thông tin mạng liên quan đến việc kết nối vào Trung tâm tích hợp dữ liệu của tỉnh.

3. Các cơ quan, đơn vị khi kết nối vào Trung tâm tích hợp dữ liệu phải bảo vệ thiết bị đầu cuối của mình, chịu trách nhiệm nếu để tin tặc kiểm soát máy tính và truy cập trái phép vào Trung tâm tích hợp dữ liệu của tỉnh.

Điều 6. Phát triển nguồn nhân lực an toàn thông tin

1. Cán bộ chuyên trách về công nghệ thông tin trong các cơ quan, đơn vị được tạo điều kiện trang bị các thiết bị tin học, phương tiện kỹ thuật làm việc phù hợp với chuyên môn; tham dự đầy đủ các khóa đào tạo và bồi dưỡng kiến thức, nghiệp vụ cho cán bộ quản lý, kỹ thuật về an toàn thông tin mạng.

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

Chương III
TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 7. Sở Thông tin và Truyền thông

1. Tham mưu UBND tỉnh về chỉ đạo, triển khai công tác 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 Quảng Nam.

2. Là đầu mối phối hợp với các cơ quan bảo đảm an toàn thông tin của Trung ương và địa phương khác để xử lý, ứng cứu các sự cố an toàn thông tin mạng trên địa bàn tỉnh. Hướng dẫn cụ thể về nghiệp vụ quản lý, vận hành, kỹ thuật bảo đảm an toàn thông tin, đồng thời, hỗ trợ các cơ quan, đơn vị giải quyết sự cố an toàn thông tin mạng khi có yêu cầu.

3. Tập hợp đội ngũ cán bộ chuyên trách về an toàn thông tin có trình độ đáp ứng yêu cầu nhiệm vụ; tổ chức bộ phận chuyên trách về an toàn thông tin có trách nhiệm bảo đảm an toàn thông tin mạng cho các hệ thống công nghệ thông tin dùng chung của tỉnh và hỗ trợ các cơ quan, đơn vị trong tỉnh xử lý sự cố an toàn thông tin mạng.

4. Hằng năm, xây dựng kế hoạch, lập dự toán kinh phí trình cấp có thẩm quyền phê duyệt để triển khai công tác bảo đảm an toàn thông tin, hoạt động của Ban Chỉ đạo Công nghệ thông tin tỉnh, đơn vị chuyên trách ứng cứu sự cố (Sở Thông tin và Truyền thông), Đội ứng cứu sự cố như: Thuê, mua thiết bị phần cứng, phần mềm, cơ sở vật chất để phục vụ hoạt động ứng cứu sự cố mạng; kinh phí triển khai ứng cứu, xử lý sự cố cho các hệ thống thông tin của tỉnh; kinh phí tổ chức đào tạo kiến thức về công nghệ thông tin, huấn luyện, diễn tập và hoạt động của Đội ứng cứu sự cố; kinh phí kiểm tra, giám sát, rà quét, đánh giá an toàn thông tin cho các hệ thống thông tin thuộc phạm vi tỉnh quản lý.

5. Có trách nhiệm lập và tổng hợp kinh phí trong việc thực hiện các hoạt động ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh để thanh quyết toán theo phân cấp ngân sách quy định tại Luật Ngân sách và các văn bản hướng dẫn thi hành.

6. Chủ trì, phối hợp với các cơ quan liên quan thành lập Đoàn kiểm tra an toàn thông tin mạng định kỳ hàng năm hoặc kiểm tra đột xuất khi phát hiện có các dấu hiệu vi phạm an toàn thông tin mạng.

7. Chịu trách nhiệm xây dựng và trình UBND tỉnh ban hành các cơ chế, chính sách và hướng dẫn, khuyến nghị về bảo đảm an toàn thông tin mạng cho các cơ quan, đơn vị.

8. Hướng dẫn, giám sát các đơn vị xây dựng quy chế, quy trình bảo đảm an toàn cho hệ thống thông tin theo quy định của nhà nước; thông báo cho các cơ quan, đơn vị biết và có biện pháp phòng ngừa, ngăn chặn các nguy cơ mất an toàn thông tin mạng.

9. Thẩm định về an toàn thông tin mạng trong hồ sơ thiết kế hệ thống thông tin trong các cơ quan nhà nước trên địa bàn tỉnh.

10. Xây dựng và triển khai các chương trình đào tạo, tổ chức các hội nghị, hội thảo về an toàn thông tin mạng nhằm phổ biến, cập nhật kiến thức về an toàn thông tin.

11. Thông báo cho các cơ quan, đơn vị biết và có biện pháp phòng ngừa, ngăn chặn rủi ro an toàn thông tin mạng, các nguy cơ mất an toàn thông tin do virus, phần mềm độc hại, phần mềm gián điệp gây ra.

Điều 8. Công an tỉnh

1. Điều tra và xử lý các trường hợp vi phạm an toàn thông tin mạng theo thẩm quyền.

2. Phối hợp với Sở Thông tin và Truyền thông thanh tra, kiểm tra công tác bảo đảm an toàn thông tin mạng đối với các cơ quan, đơn vị trên địa bàn tỉnh.

3. Kịp thời thông báo, trao đổi với các cơ quan, đơn vị về phương thức, thủ đoạn mới của các loại tội phạm xâm phạm an toàn, an ninh thông tin để có biện pháp phòng ngừa, đấu tranh, ngăn chặn.

4. Thực hiện nhiệm vụ bảo vệ an toàn các công trình quan trọng về an ninh quốc gia; hạ tầng cơ sở lĩnh vực công nghệ thông tin trên địa bàn tỉnh.

Điều 9. Sở, Ban, ngành, đoàn thể; UBND các huyện, thị xã, thành phố

1. Thủ trưởng các cơ quan, đơn vị có trách nhiệm tổ chức quán triệt, nâng cao nhận thức cho cán bộ, công chức, viên chức về đảm bảo an toàn thông tin mạng; tổ chức triển khai thực hiện các quy định tại Quy chế này và chịu trách nhiệm trước UBND tỉnh trong công tác bảo đảm an toàn thông tin mạng của cơ quan, đơn vị mình.

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

3. Phân công lãnh đạo phụ trách và thành lập hoặc chỉ định bộ phận đầu mối chịu trách nhiệm về an toàn thông tin mạng của cơ quan, đơn vị.

4. Xây dựng nội dung, lập dự toán kinh phí lồng ghép trong Kế hoạch ứng dụng công nghệ thông tin hàng năm của cơ quan, đơn vị mình để triển khai các nhiệm vụ bảo đảm và tăng cường an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin.

5. Khi có sự cố an toàn thông tin mạng hoặc có nguy cơ mất an toàn thông tin mạng phải kịp thời chỉ đạo cán bộ kỹ thuật chuyên trách trong cơ quan, đơn vị khắc phục ngay; báo cho doanh nghiệp cung cấp dịch vụ và thông báo bằng văn bản cho Sở Thông tin và Truyền thông, cơ quan cấp trên quản lý trực tiếp biết. Trong trường hợp không khắc phục được thì phối hợp với Sở Thông tin và Truyền thông hoặc cơ quan cấp trên quản lý để được hướng dẫn, hỗ trợ.

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

7. Trên cơ sở hướng dẫn của Sở Thông tin và Truyền thông, xây dựng và ban hành quy định cụ thể về bảo đảm an toàn thông tin mạng; phương án thực hiện bảo vệ hệ thống thông tin mạng trong cơ quan, đơn vị mình.

8. Khi triển khai đầu tư ứng dụng công nghệ thông tin 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 mạng cho hệ thống công nghệ thông tin và các hệ thống thông tin của cơ quan, đơn vị mình.

9. Phối hợp với Sở Thông tin và Truyền thông và các cơ quan, đơn vị liên quan thực hiện công tác kiểm tra khắc phục sự cố an toàn thông tin mạng. Không che dấu thông tin về sự cố an toàn thông tin nhằm gây khó khăn cho các cơ quan chức năng trong quá trình đánh giá thiệt hại để có phương án xử lý kịp thời, hiệu quả.

10. Định kỳ 06 tháng và hằng năm (trước ngày 15/11), gửi báo cáo tình hình, kết quả thực hiện công tác đảm bảo an toàn thông tin mạng tại cơ quan, đơn vị mình về Sở Thông tin và Truyền thông để tổng hợp báo cáo UBND tỉnh.

Điều 10. Sở Tài chính, Sở Kế hoạch và Đầu tư

Phối hợp với Sở Thông tin và Truyền thông tham mưu UBND tỉnh trong việc bố trí kinh phí cho các hoạt động đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh.

Điều 11. Các doanh nghiệp tư vấn, cung cấp dịch vụ viễn thông, CNTT và Internet cho các cơ quan quản lý nhà nước tỉnh Quảng Nam

1. Tư vấn và cung cấp trang bị hạ tầng kỹ thuật đáp ứng đầy đủ các yêu cầu, tiêu chuẩn kỹ thuật theo quy định của Bộ Thông tin và Truyền thông về an ninh mạng, an toàn thông tin và các nội dung quy định tại Quy chế này.

2. Phối hợp với Sở Thông tin và Truyền thông để tham gia các hoạt động điều phối, ứng cứu, khắc phục sự cố thông tin bảo đảm an toàn thông tin mạng cho các cơ quan, đơn vị trong quá trình sử dụng, khai thác dịch vụ.

Điều 12. Cán bộ, công chức, viên chức, người lao động trong các cơ quan, đơn vị

1. Trách nhiệm của cán bộ chuyên trách hoặc cán bộ được giao phụ trách công nghệ thông tin trong các cơ quan, đơn vị

a) Chịu trách nhiệm đảm bảo an toàn thông tin mạng của đơn vị.

b) Chịu trách nhiệm triển khai các biện pháp kỹ thuật, quản lý, vận hành, 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.

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

d) Tham gia đầy đủ các khóa đào tạo, tập huấn, bồi dưỡng về bảo đảm an