ỦY BAN NHÂN DÂN TỈNH ĐẮK NÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 20/2017/QĐ-UBND	*Đắk Nông, ngày 23 tháng 8 năm 2017*

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 nhà nước trên địa bàn tỉnh Đắk Nông

ỦY BAN NHÂN DÂN TỈNH ĐẮK NÔNG

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

Căn cứ Luật Ban hành văn bản quy phạm pháp luật ngày 22/6/2015;

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

Căn cứ Luật An toàn an ninh 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 72/2013/NĐ-CP ngày 15/7/2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin mạng;

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

Căn cứ Nghị định số 142/2016/NĐ-CP ngày 14/10/2016 của Chính phủ về ngăn chặn xung động thông tin trên mạng;

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 của Bộ Thông tin và Truyền thông 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;

Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Tờ trình số 31/TTr-STTTT ngày 03/7/2017.

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 cơ quan nhà nước trên địa bàn tỉnh Đắk Nông.

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày 05/9/2017.

Quyết định này thay thế Quyết định số 28/2010/QĐ-UBND ngày 28/9/2010 của Ủy ban nhân dân tỉnh về việc ban hành Quy chế đảm bảo an toàn, an ninh thông tin trong lĩnh vực ứng dụng công nghệ thông tin của các cơ quan, đơn vị quản lý hành chính nhà nước trên địa bàn tỉnh Đắk Nông.

Điều 3. Chánh Văn phòng Ủy ban nhân dân tỉnh; Thủ trưởng các Sở, Ban, ngành; Chủ tịch Ủy ban nhân dân các huyện, thị xã; Chủ tịch Ủy ban nhân dân xã, phường, thị trấn 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;
- Cục Kiểm tra văn bản (Bộ Tư pháp);
- Thường trực Tỉnh ủy;
- Thường trực HĐND tỉnh;
- CT, các PCT UBND tỉnh;
- Ủy ban MTTQ Việt Nam tỉnh;
- Ban Tuyên giáo Tỉnh ủy;
- Ban Nội chính Tỉnh ủy;
- Văn phòng Đoàn ĐBQH tỉnh;
- Văn phòng HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các thành viên BCĐ CCHC tỉnh;
- Báo Đắk Nông, Đài PT-TH tỉnh;
- Công báo tỉnh;
- Cổng TTĐT tỉnh Đắk Nông;
- Chi Cục Văn thư - Lưu trữ tỉnh;
- Lưu: VT, NC, CNXD, KGVX (Q)

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Người ký: Ủy ban Nhân dân tỉnh Đắk Nông
Thời gian ký: 24.08.2017 15:13:35 +07:00

Nguyễn Bốn

ỦY BAN NHÂN DÂN TỈNH ĐẮK NÔNG	CỘNG HÒA 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 nhà nước trên địa bàn tỉnh Đắk Nông

(Ban hành kèm theo Quyết định số 20 /2017/QĐ-UBND ngày 23 tháng 8 năm 2017 của Ủy ban nhân dân tỉnh Đắk Nông)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về công tác bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin (CNTT) của các cơ quan nhà nước trên địa bàn tỉnh Đắk Nông (*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 nhà nước và các đối tượng có liên quan trên địa bàn tỉnh Đắk Nông, bao gồm:

a) Các Sở, Ban, ngành và các đơn vị trực thuộc;

b) Các đơn vị sự nghiệp công lập thuộc Ủy ban nhân dân tỉnh;

c) Ủy ban nhân dân các huyện, thị xã và các đơn vị trực thuộc;

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

đ) Các doanh nghiệp cung cấp dịch vụ viễn thông, công nghệ thông tin, Internet; Các doanh nghiệp, tổ chức, cá nhân tham gia vào hoạt động ứng dụng công nghệ thông tin của cơ quan 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. Khuyến khích các cơ quan, đơn vị khác hoạt động ứng dụng và phát triển CNTT trên địa bàn tỉnh áp dụng quy chế này.

Điều 3. Giải thích từ ngữ

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

1. An toàn thông tin mạng: Là sự bảo vệ thông tin, hệ thống thông tin trên mạng 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.

2. Mạng: Là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua mạng viễn thông và mạng máy tính.

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

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

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

6. Tính toàn vẹn: bảo vệ tính chính xác và tính đầy đủ của thông tin và các phương pháp xử lý thông tin.

7. Tính tin cậy: Bảo đảm thông tin chỉ có thể được truy cập bởi những người được cấp quyền sử dụng.

8. Tính sẵn sàng: Bảo đảm những người được cấp quyền có thể truy cập thông tin và các tài nguyên (mạng, máy chủ, tên miền, tài khoản thư điện tử…) ngay khi có nhu cầu.

9. Logfile: Là một tập tin ghi lại các sự kiện xảy ra trong hệ điều hành hoặc các phần mềm trong quá trình hoạt động.

10. Máy chủ ảo: Là dạng máy chủ được tạo ra bằng phương pháp phân chia một máy chủ vật lý thành nhiều máy chủ khác nhau bằng công nghệ ảo hóa, máy chủ ảo chạy dưới dạng chia sẻ tài nguyên từ máy chủ vật lý ban đầu.

11. Mạng nội bộ: Là mạng máy tính trong phạm vi trụ sở của một cơ quan, đơn vị.

12. Mạng riêng ảo (VPN - Virtual Private Network): Là một mạng máy tính dành riêng để kết nối các máy tính của các cơ quan nhà nước với nhau thông qua mạng Internet.

13. Thiết bị di động: Các thiết bị di động cá nhân có kết nối vào mạng nội bộ của cơ quan nhà nước như máy tính xách tay, máy tính bảng, điện thoại di động, các thiết bị di động khác.

Điều 4. Nguyên tắc chung

1. Việc bảo đảm an toàn, an ninh thông tin 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, an ninh 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, an ninh thông tin.

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, an ninh thông tin.

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, an ninh thông tin.

6. Các văn bản có nội dung "Mật" trở lên khi gửi, nhận qua mạng phải được thủ trưởng cơ quan, đơn vị cho phép và phải được mã hóa theo quy định của Luật cơ yếu và các văn bản pháp luật liên quan.

Chương II
QUY ĐỊNH BẢO ĐẢM AN TOÀN, AN NINH THÔNG TIN

Điều 5. Quản lý tài sản 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. Trước khi đưa vào sử dụng, đơn vị có thể đề nghị cơ quan công an chủ trì, phối hợp với Sở Thông tin và Truyền thông, đơn vị quân đội và đơn vị tư vấn giám sát kiểm tra, đánh giá đối với các thiết bị CNTT sử dụng tại các cơ quan trọng yếu, phục vụ các công việc yêu cầu bảo đảm bí mật.

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. Phân loại tài sản công nghệ thông tin (vật lý, thông tin, dữ liệu) theo mức độ giá trị, độ nhạy cảm, tầm ảnh hưởng đối với hệ thống, tần suất sử dụng, thời gian lưu trữ để xây dựng nội quy, biện pháp kỹ thuật nghiệp vụ phù hợp (định kỳ sao lưu dữ liệu, bảo trì hệ thống...).

5. 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.

6. 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 hủy bỏ thông tin, dữ liệu để tránh lộ, lọt thông tin bí mật, mất dữ liệu và phải bảo đảm không thể phục hồi.

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

1. Các cơ quan, đơn vị thường xuyên tổ chức quán triệt các quy định về an toàn thông tin nhằm nâng cao nhận thức về trách nhiệm bảo đảm an toàn, an ninh thông tin 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 định bảo đảm an toàn, an ninh thông tin 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 công tác bảo đảm an toàn, an ninh thông tin, quản trị hệ thống CNTT của cơ quan, đơn vị.

4. Các cơ quan, đơn vị 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 mạng, an toàn, an ninh thông tin; đồng thời, phổ biến, cập nhật các quy chế về an toàn, an ninh thông tin hàng năm để mọi người hiểu rõ các quyền và trách nhiệm đối với việc bảo đảm an toàn thông tin. Thường xuyên kiểm tra việc thực hiện các nội quy, quy định về an toàn, an ninh thông tin của đơn vị đối với cán bộ, công chức, viên chức, người lao động theo định kỳ.

5. 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 vào ra thích hợp, bảo đảm chỉ những người có nhiệm vụ mới được vào khu vực đó;

b) Phòng đặt thiết bị CNTT (đối với các cơ quan, đơn vị đang quản lý, vận hành các hệ thống thông tin, cơ sở dữ liệu của tỉnh) phải bảo đảm các điều kiện đáp ứng các yêu cầu cơ bản (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 nguồn điện dự phòng; có bình chữa cháy hoặc hệ thống tự động cảnh báo, chữa cháy khẩn cấp; phòng, chống sét; có nội quy, quy trình làm việc trong khu vực an toàn bảo mật). Phải thiết lập cơ chế bảo vệ mạng nội bộ, bảo đảm an toàn thông tin khi có kết nối với mạng ngoài bằng các công cụ, thiết bị bảo vệ (tường lửa, hệ thống chống xâm nhập trái phép, hệ thống giám sát, cảnh báo sớm);

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 chống cháy nổ, 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. Các thiết bị CNTT 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 bảo đảm 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 (password) cho người được giao sử dụng để bảo đảm an toàn, bảo mật thông tin.

4. Kiểm soát chặt chẽ việc cài đặt các phần mềm mới lên máy chủ, máy trạm và các thiết bị di động. Các phần mềm được cài đặt trên máy chủ, máy trạm và các thiết bị di động (bao gồm hệ điều hành, các phần mềm ứng dụng văn phòng, phần mềm phục vụ công việc, tiện ích khác) phải được thường xuyên theo dõi, cập nhật bản vá lỗi bảo mật của nhà phát triển, lựa chọn cài đặt các phần mềm chống, diệt virus, mã độc và thường xuyên cập nhật phiên bản mới, đặt lịch quét virus theo định kỳ ít nhất hàng tuần.

5. Cơ quan nhà nước phải quy định cụ thể về quản lý, vận hành sử dụng máy chủ, quản lý chặt chẽ logfile để ghi nhận thông tin quá trình đăng nhập hệ thống, các thay đổi, cấu hình hệ thống, theo dõi các dịch vụ, sự kiện trong quá trình vận hành máy chủ. Chỉ cài đặt các phần mềm cần thiết, không được cài đặt các phần mềm bẻ khóa, tắt các dịch vụ, các port (cổng) không sử dụng; chia sẻ tài nguyên trên máy chủ phải được phân quyền khoa học, rõ ràng.

6. 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.

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

8. 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.

9. Quản lý hệ thống mạng nội bộ: Mạng nội bộ của các cơ quan nhà nước phải được tổ chức theo mô hình Clients/Server; mạng nội bộ khi kết nối với mạng Internet phải thông qua thiết bị tường lửa kiểm soát (tường lửa phải thường xuyên được cập nhật dữ liệu theo hướng dẫn, yêu cầu của nhà sản xuất), có phân chia hệ thống mạng nội bộ thành các vùng mạng theo phạm vi truy cập, vô hiệu hóa tất cả các dịch vụ không sử dụng tại từng vùng mạng, thực hiện nguyên tắc chỉ mở các dịch vụ cần thiết khi có yêu cầu.

10. Quản lý truy cập từ xa vào mạng nội bộ: Đối với việc truy cập từ xa vào mạng nội bộ phải được theo dõi, quản lý chặt chẽ, nhất là truy cập có sử dụng chức năng quản trị, phải thiết lập mật mã độ an toàn cao, nhắc nhở khuyến cáo thường xuyên thay đổi mật mã, tăng cường sử dụng mạng riêng ảo, hạn chế truy cập từ xa vào mạng nội bộ từ các điểm truy cập Internet công cộng.

11. 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 (khu vực không bảo mật), thiết bị không dây cần được 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, thường xuyên thay đổi mật khẩu nhằm tăng cường công tác bảo mật.

12. Tất cả máy chủ, máy trạm phải được thiết lập mật mã truy cập và chế độ tự động bảo vệ màn hình sau 10 phút không sử dụng. Mật mã đăng nhập, truy cập hệ thống thông tin phải có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số hoặc ký tự đặc biệt như: !, @, #, $, %,...) và phải được thay đổi ít nhất 03 tháng/01lần.

13. Đối với các cơ quan nhà nước có sử dụng đường truyền Internet ngoài đường truyền số liệu chuyên dùng trong hệ thống các cơ quan Đảng, Nhà nước, phải thông báo về Sở Thông tin và Truyền thông để được hướng dẫn đấu nối, thiết lập các thông số của các thiết bị định tuyến, cấu hình địa chỉ IP cho hệ thống mạng nội bộ, các máy chủ, máy trạm trong cơ quan thống nhất với toàn hệ thống.

14. Chống mã độc, virus và các hình thức xâm nhập khác: Lựa chọn, triển khai các thiết bị phần cứng và phần mềm chống xâm nhập (Firewall), 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.

15. 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.

16. Chỉ tiếp nhận và đưa vào vận hành hệ thống thông tin sau khi đã thực hiện nghiệm thu và kiểm thử hệ thống (được thẩm định, xác nhận của bộ phận chuyên trách và phê duyệt của cơ quan, đơn vị có thẩm quyền của Sở Thông tin và Truyền thông, Bộ Thông tin và Truyền thông hoặc chủ quản hệ thống thông tin).

17. Xem xét tính tương thích của phần mềm, ứng dụng hiện có, bảo đảm hoạt động ổn định, an toàn trước khi quyết định thay đổi hoặc nâng cấp hệ điều hành lên phiên bản mới hơn; kiểm soát chặt chẽ việc nâng cấp, mở rộng phần mềm, ứng dụng trong hệ thống. Việc bổ sung các thiết bị vào hệ thống thông tin cần có kế hoạch, quy trình bảo đảm việc tiếp nhận không làm gián đoạn hoạt động của hệ thống đang vận hành; bảo trì hệ thống thông tin phải có kế hoạch từ trước và được thực hiện thường xuyên.

18. Các cơ quan, đơn vị trong phạm vi quyền hạn của mình có trách nhiệm ngăn chặn xung đột thông tin trên mạng theo các nội dung quy định tại khoản 1 Điều 28 Luật an toàn thông tin mạng; khoản 1 Điều 8; khoản 1, Điều 9; các khoản 3, 4, 5 Điều 12; các khoản 1, 2 Điều 14 và Điều 27 Nghị định số 142/2016/NĐ-CP ngày 14/10/2016 của Chính phủ và các quy định sau:

a) Phải thực hiện các biện pháp bảo vệ hệ thống thông tin của mình quản lý, không để các phần tử xấu lợi dụng hệ thống thông tin để thâm nhập, truy cập trái phép vào các trung tâm đang quản lý các hệ thống thông tin, cơ sở dữ liệu của tỉnh;

b) Cán bộ, công chức của các cơ quan, đơn vị có trách nhiệm ngăn chặn xung đột thông tin trên mạng theo các nội dung quy định tại khoản 1 Điều 28 Luật an toàn thông tin mạng; khoản 1 Điều 7; các khoản 4, 5 Điều 12 và Điều 27 Nghị định số 142/2016/NĐ-CP ngày 14/10/2016 của Chính phủ.

Điều 8. Quy định đối với bên thứ ba khi tham gia vào hệ thống an toàn an ninh thông tin

1. 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 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 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 định an toàn, an ninh 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 cơ quan, đơn vị;

đ) Khi phát hiện bên thứ ba có dấu hiệu vi phạm hoặc vi phạm quy chế an toàn, bảo mật thông tin của bên thứ ba thì cơ quan, đơn vị phải: Tạm dừng hoặc đình chỉ hoạt động của bên thứ ba tùy theo mức độ vi phạm; thông báo chính thức các vi phạm về an toàn, bảo mật CNTT của nhân sự cho bên thứ ba; kiểm tra xác định, lập báo cáo mức độ vi phạm và thông báo cho bên thứ ba thiệt hại xảy ra; thu hồi ngay quyền truy cập hệ thống CNTT đã được cấp cho bên thứ ba;

e) Sau khi kết thúc công việc, phải thu hồi quyền truy cập hệ thống CNTT đã được cấp của bên thứ ba; thay đổi các khóa, mật khẩu nhận bàn giao từ bên thứ ba.

2. Trách nhiệm của bên thứ ba trong quá trình triển khai cơ quan, đơn vị cần:

a) Cung cấp danh sách nhân sự tham gia và ký cam kết không tiết lộ thông tin của cơ quan, đơn vị đối với các thông tin quan trọng;

b) Tuân thủ đầy đủ các quy định về an toàn thông tin và giám sát quá trình khi triển khai thực hiện hệ thống CNTT tại cơ quan, đơn vị;

c) Sau khi kết thúc công việc: phải bàn giao lại tài sản sử dụng của đơn vị trong quá trình triển khai công việc, tài khoản, quyền truy cập hệ thống CNTT đã được cấp khi tham gia vào hệ thống CNTT tại cơ quan, đơn vị.

Điều 9. Bảo đảm an toàn, an ninh 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 mang 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.

7. Cơ quan nhà nước rà soát tối thiểu 03 tháng/01 lần các tài khoản đăng nhập, bảo đảm các tài khoản và quyền truy cập hệ thống được cấp phát đúng, đủ. Khi người dùng thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ hưu thì cơ quan nhà nước phải kịp thời thông báo cho Sở Thông tin và Truyền thông thu hồi tài khoản được cấp (đối với các hệ thống do Sở Thông tin và Truyền thông quản lý tập trung tại Trung tâm tích hợp dữ liệu tỉnh).

8. Đối với bên thứ ba:

a) Thực hiện giám sát và kiểm tra các dịch vụ do bên thứ ba cung cấp bảo đảm mức độ cung cấp dịch vụ, khả năng hoạt động hệ thống đáp ứng đúng theo thỏa thuận đã ký kết;

b) Bảo đảm triển khai, duy trì các biện pháp an toàn, bảo mật của dịch vụ do bên thứ ba cung cấp theo đúng thỏa thuận;

c) Quản lý các thay đổi đối với các dịch vụ của bên thứ ba cung cấp bao gồm: Nâng cấp phiên bản mới; sử dụng các kỹ thuật mới, các công cụ và môi trường phát triển mới;

d) Đánh giá đầy đủ tác động của việc thay đổi, bảo đảm an toàn khi được đưa vào sử dụng.

Điều 10. Quản lý, khắc phục sự cố, lưu trữ và dự phòng

1. Các sự kiện, sự cố về an toàn, an ninh thông tin 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, an ninh 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. 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, an ninh thông tin 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 *(theo Phụ lục 02)*.

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, an ninh thông tin 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.

Điều 11. Bảo đảm an toàn, an ninh thông tin 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 đơn vị tham gia phải tuân thủ các quy chế về bảo đảm an toàn, an ninh thông tin 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) Mạng nội bộ, mạng diện rộng, mạng truyền số liệu chuyên dùng;

đ) Hệ thống cơ sở dữ liệu, trung tâm dữ liệu, điện toán đám mây;

e) Hệ thống xác thực điện tử, chứng thực điện tử, chữ ký số;

g) Hệ thống họp, hội nghị truyền hình trực tuyến;

h) 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 và dịch vụ công trực tuyến;

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, an ninh thông tin 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.

3. Trong trao đổi thông tin, dữ liệu phục vụ công việc, cơ quan nhà nước, cán bộ công chức, viên chức phải sử dụng hệ thống thông tin do cơ quan nhà nước có thẩm quyền triển khai như: hệ thống thư điện tử công vụ tỉnh (*@daknong.gov.vn*), phần mềm quản lý văn bản và điều hành, hệ thống họp giao ban trực tuyến,... Hạn chế việc sử dụng các phương tiện trao đổi thông tin dữ liệu, hệ thống thư điện tử, lưu trữ điện tử công cộng, mạng xã hội trên Internet trong hoạt động của cơ quan nhà nước.

Điều 12. Ban hành và triển khai quy chế bảo đảm an toàn, an ninh thông tin tại cơ quan, đơn vị, địa phương

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

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 13. Trách nhiệm của cán bộ, công chức, viên chức và người lao động trong các cơ quan, đơn vị, địa phương

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

a) Chịu trách nhiệm đảm bảo an toàn, an ninh thông tin 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, an ninh thông tin;

c) Thực hiện việc giám sát, đánh giá, báo cáo Thủ trưởng cơ quan, đơn vị các rủi ro mất an toàn, an ninh 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;

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

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

a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về an toàn, an ninh thông tin. Chịu trách nhiệm đảm bảo an toàn, an ninh thông tin 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, an ninh thông tin 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, an ninh thông tin được tỉnh hoặc đơn vị chuyên môn tổ chức.

Điều 14. Trách nhiệm của các cơ quan, đơn vị, địa phương

1. Thủ trưởng các cơ quan, đơn vị, địa phương 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, an ninh thông tin của cơ quan, đơn vị, địa phương mình.

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

3. Xây dựng quy chế, quy trình về bảo đảm an toàn, an ninh thông tin phù hợp với quy định tại Điều 12, Quy chế này và các quy định của pháp luật; đưa nội dung thực hiện bảo đảm an toàn thông tin vào kế hoạch ứng dụng công nghệ thông tin hàng năm của cơ quan, đơn vị.

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. 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, an ninh thông tin.

6. Hàng năm bố trí kinh phí cho việc ứng dụng công nghệ thông tin nói chung và công tác bảo đảm an toàn, an ninh thông tin nói riêng trong nội bộ cơ quan, đơn vị, địa phương mình.

7. Phân loại thông tin và hệ thống thông tin, xây dựng phương án đảm bảo an toàn hệ thống thông tin theo cấp độ được quy định tại Điều 9, Điều 14 Thông tư 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

8. Chủ tịch UBND cấp huyện có trách nhiệm chỉ đạo các phòng, ban chuyên môn và UBND cấp xã thuộc phạm vi quản lý tổ chức thực hiện quy chế này.

9. Báo cáo tình hình, kết quả thực hiện công tác bảo đảm an toàn thông tin tại cơ quan, đơn vị, địa phương và gửi về Sở Thông tin và Truyền thông định kỳ mỗi năm 02 lần vào trước ngày 15 tháng 6 và ngày 15 tháng 12 hàng năm (hoặc đột xuất) theo biểu mẫu tại Phụ lục 01 Quy chế này, làm cơ sở để Sở Thông tin và Truyền thông tổng hợp, báo cáo Ủy ban nhân dân tỉnh và Bộ Thông tin và Truyền thông.

Điều 15. Trách nhiệm của Sở Thông tin và Truyền thông

1. Tham mưu Ủy ban nhân dân tỉnh về công tác bảo đảm an toàn thông tin trong các cơ quan nhà nước tỉnh và chịu trách nhiệm trước Ủy ban nhân dân tỉnh trong việc bảo đảm an toàn cho các hệ thống thông tin dùng chung của tỉnh như: Cổng thông tin điện tử, Thư điện tử, Giao ban điện tử và các hệ thống thông tin dùng chung khác của tỉnh.

2. Chịu trách nhiệm xây dựng, trình Ủy ban nhân dân tỉnh hoặc tham mưu Ủy ban nhân dân tỉnh trình Hội đồng nhân dân tỉnh ban hành các cơ chế, chính sách và hướng dẫn, khuyến nghị về đảm bảo an toàn thông tin mạng cho các cơ quan, đơn vị.

3. Tham mưu Ủy ban nhân dân tỉnh xây dựng đội ngũ cán bộ chuyên trách về an toàn thông tin có trình độ đáp ứng yêu cầu theo quy định; tổ chức bộ phận chuyên trách về an toàn thông tin có trách nhiệm đảm bảo an toàn thông tin cho các hệ thống CNTT dùng chung của tỉnh và hỗ trợ các cơ quan, đơn vị trong tỉnh xử lý sự cố an toàn thông tin mạng.

4. Chủ trì, phối hợp với Công an tỉnh và các cơ quan, đơn vị có liên quan định kỳ hàng năm tiến hành công tác thanh tra, kiểm tra, đánh giá công tác bảo đảm an toàn thông tin và xử lý các hành vi vi phạm an toàn thông tin mạng tại các cơ quan nhà nước trên địa bàn tỉnh. Tổ chức kiểm tra đột xuất các cơ quan đơn vị khi có dấu hiệu vi phạm an toàn thông tin mạng.

5. Hàng năm, xây dựng kế hoạch, chương trình, dự án, tổng hợp kinh phí để triển khai công tác an toàn thông tin trong hoạt động ứng dụng CNTT của các cơ quan, đơn vị trên địa bàn tỉnh.

6. Thẩm định về an toàn thông tin mạng trong hồ sơ thiết kế hệ thống thông tin trong của các cơ quan, đơn vị trên địa bàn tỉnh.

7. Tổ chức thẩm định hồ sơ đề xuất cấp độ về bảo đảm an toàn hệ thống thông tin theo cấp độ 1, 2, 3 được quy định tại khoản 1, Điều 15, Thông tư 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

8. Đầu mối đơn vị chuyên trách về an toàn thông tin của tỉnh Đắk Nông trình Bộ Thông tin và Truyền thông thẩm định hồ sơ được đề xuất cấp độ 4, 5 được quy định tại khoản 2, Điều 15, Thông tư Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông 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.

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

10. 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.

11. Thực hiện nhiệm vụ cảnh báo về nguy cơ hoặc sự cố mất an toàn thông tin mạng; tiếp nhận thông tin, hỗ trợ kỹ thuật và tham gia xử lý các sự cố về an toàn thông tin mạng cho các cơ quan, đơn vị. Tổ chức thực hiện các hoạt động điều phối của Đội ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh và các nhiệm vụ được quy định tại khoản 2, 3 Điều 6; các khoản 2, 3 Điều 9; khoản 3, Điều 14; các khoản 1, 3 Điều 15 và Điều 16, 17, 18 của Nghị định số 142/2016/NĐ-CP ngày 14/10/2016 của Chính phủ.

12. 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.

13. Phối hợp với Cục An toàn thông tin, Trung tâm ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) và các tổ chức, đơn vị liên quan trong hoạt động liên quan đến công tác bảo đảm an toàn thông tin mạng.

14. Định kỳ 6 tháng, hàng năm hoặc đột xuất tổng hợp báo cáo Ủy ban nhân dân tỉnh về tình hình bảo đảm an toàn thông tin mạng trong các cơ quan nhà nước tỉnh Đắk Nông.

15. Trung tâm Công nghệ thông tin và Truyền thông trực thuộc Sở Thông tin và Truyền thông là đơn vị trực tiếp vận hành kỹ thuật Trung tâm tích hợp dữ liệu tỉnh, phải chịu trách nhiệm ban hành quy chế nội bộ theo các nội dung của Quy chế này và Quy chế quản lý, vận hành, khai thác Trung tâm tích hợp dữ liệu tỉnh, các tiêu chuẩn quốc gia và tham khảo các tiêu chuẩn quốc tế về an toàn thông tin.

Điều 16. 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 xây dựng kế hoạch để ngăn chặn, kiểm soát, phòng ngừa, đấu tranh,

các loại tội phạm lợi dụng hệ thống mạng gây hại đến an toàn, an ninh thông tin trong cơ quan nhà nước.

2. Phối hợp với các cơ quan có liên quan tham mưu Ủy ban nhân dân tỉnh hướng dẫn việc sử dụng các thiết bị CNTT để lưu giữ và truyền tải thông tin bí mật nhà nước. Hỗ trợ các cơ quan, đơn vị thực hiện việc kiểm tra, đánh giá nguy cơ mất an toàn, an ninh thông tin khi có yêu cầu.

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

Điều 17. Trách nhiệm của Sở Tài chính, Sở Kế hoạch và Đầu tư

1. Phối hợp với Sở Thông tin và Truyền thông tham mưu Ủy ban nhân dân tỉnh bố trí kinh phí sự nghiệp hàng năm và kinh phí thực hiện các nhiệm vụ đột xuất phục vụ việc mua sắm máy móc, thiết bị, nâng cấp hạ tầng máy chủ, máy trạm, hệ thống tường lửa, kinh phí đào tạo, tập huấn cho các bộ chuyên trách công nghệ thông tin, kinh phí ứng cứu sự cố an toàn thông tin mạng... bảo đảm cho các hoạt động an toàn, an ninh thông tin trong hoạt động ứng dụng CNTT cho các cơ quan, đơn vị trên địa bàn tỉnh.

2. Hướng dẫn mục chi cho công tác bảo đảm an toàn thông tin trong dự toán ngân sách, hướng dẫn quản lý và sử dụng kinh phí sự nghiệp chi cho công tác bảo đảm an toàn thông tin trong hoạt động của các cơ quan, tổ chức nhà nước.

3. Chủ trì, phối hợp với Sở Thông tin và Truyền thông tổng hợp, tham mưu ưu tiên bố trí nguồn vốn ngân sách trong kế hoạch chi đầu tư phát triển hàng năm để thực hiện các dự án đầu tư bảo đảm an toàn thông tin mạng cho các cơ quan, đơn vị.

Điều 18. Trách nhiệm của Ban chỉ đạo Cải cách hành chính tỉnh

1. Chỉ đạo công tác điều phối, ứng cứu sự cố trong hoạt động ứng dụng CNTT trên địa bàn tỉnh; chỉ đạo các cơ quan, đơn vị trên địa bàn tỉnh phối hợp, tuân thủ yêu cầu của Cơ quan điều phối quốc gia, Đội ứng cứu sự cố mạng máy tính tỉnh trong điều phối, ứng cứu sự cố.

2. Triệu tập, chỉ đạo bộ phận tác nghiệp ứng cứu sự cố tại các cơ quan, đơn vị theo đề xuất của Đội ứng cứu sự cố mạng máy tính tỉnh.

Điều 19. Trách nhiệm của Đội ứng cứu sự cố mạng máy tính tỉnh

1. Tham mưu cho Ủy ban nhân dân tỉnh, Ban chỉ đạo Cải cách hành chính tỉnh, Sở Thông tin và Truyền thông chỉ đạo tổ chức triển khai công tác bảo đảm an toàn an ninh thông tin và ứng cứu sự cố mạng, máy tính đối với các cơ quan, đơn vị trên địa bàn tỉnh.

2. Hỗ trợ các cơ quan, đơn vị trên địa bàn tỉnh trong công tác bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng CNTT và tổ chức ứng cứu các sự cố mạng, máy tính.

3. Là cơ quan thường trực Ban chỉ đạo Cải cách hành chính tỉnh, phối hợp với Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT), các đơn vị

chức năng có liên quan ngăn chặn, xử lý và khắc phục sự cố mạng, máy tính các cơ quan, đơn vị trên địa bàn tỉnh.

4. Thực hiện trách nhiệm làm đầu mối ứng cứu sự cố của tỉnh trong mạng lưới ứng cứu sự cố mạng, máy tính trên toàn quốc dưới sự điều phối của Trung tâm ứng cứu khẩn cấp máy tính Việt Nam (VNCERT).

Điều 20. Trách nhiệm của các doanh nghiệp viễn thông, CNTT cung cấp hạ tầng phục vụ ứng dụng CNTT trong cơ quan nhà nước

1. Đầu tư xây dựng, 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 và an toàn thông tin và các nội dung quy định tại Quy chế này.

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

3. Viễn thông Đắk Nông có trách nhiệm bảo đảm hệ thống mạng truyền số liệu chuyên dùng của các cơ quan, đơn vị trên địa bàn tỉnh; phối hợp với Cục Bưu điện Trung ương, Sở Thông tin và Truyền thông trong việc xử lý khắc phục khi có sự cố trên hệ thống mạng truyền số liệu chuyên dùng của tỉnh.

Điều 21. Trách nhiệm của các tổ chức, cá nhân, doanh nghiệp tham gia quản lý, vận hành, khai thác ứng dụng CNTT trong hoạt động các cơ quan Nhà nước của tỉnh Đắk Nông

1. Xây dựng quy chế, quy định về bảo đảm an toàn thông tin mạng cho hệ thống thông tin của cơ quan, đơn vị; tham mưu xây dựng kế hoạch và tổ chức thực hiện các biện pháp bảo đảm an toàn thông tin mạng để quản lý vận hành các hệ thống thông tin.

2. Chủ động phối hợp và tuân thủ theo sự hướng dẫn kỹ thuật của Sở Thông tin và Truyền thông trong quá trình khắc phục sự cố về an toàn thông tin mạng.

3. Cử cán bộ chuyên trách an toàn thông tin tham gia đầy đủ các khóa đào tạo về bảo đảm an toàn thông tin mạng do các cơ quan chuyên môn tổ chức.

4. Thực hiện các nội dung đã được quy định tại quy chế này; các quy chế, nội quy của cơ quan, đơn vị và các quy định khác của pháp luật về an toàn thông tin mạng trong quá trình sử dụng, khai thác thông tin mạng.

5. Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo kịp thời cho lãnh đạo đơn vị để có giải pháp ngăn chặn, xử lý kịp thời.

6. Chịu trách nhiệm về các thông tin cá nhân đăng ký, khai báo khi sử dụng tương tác các ứng dụng CNTT của tỉnh; tuân thủ các hướng dẫn khi sử dụng dịch vụ CNTT của tỉnh.

7. Không thu thập, sử dụng, phát tán, quảng cáo, kinh doanh trái pháp luật thông tin cá nhân của người khác; lợi dụng sơ hở, điểm yếu của hệ thống dịch vụ ứng dụng CNTT để thu thập, khai thác thông tin cá nhân.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 22. Điều khoản thi hành

1. Thủ trưởng các Sở, Ban, ngành; Chủ tịch Ủy ban nhân dân các huyện, thị xã; Chủ tịch Ủy ban nhân dân các xã, phường, thị trấn và các cơ quan, đơn vị có liên quan chịu trách nhiệm tổ chức triển khai thực hiện Quy chế này.

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

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Nguyễn Bốn

PHỤ LỤC 1

MẪU BÁO CÁO TÌNH HÌNH AN TOÀN THÔNG TIN

(Kèm theo Quyết định số 20/2017/QĐ-UBND ngày 23/8/2017 của UBND tỉnh Đắk Nông)

UBND TỈNH ĐẮK NÔNG
TÊN ĐƠN VỊ

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Đắk Nông, ngày tháng năm 20....

BÁO CÁO TÌNH HÌNH AN TOÀN THÔNG TIN THÁNG/NĂM .....

1. Đánh giá hiện trạng và dự kiến

1. Về chính sách, quản lý

- Xây dựng quy chế nội bộ đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin:

□ Không □ Có, số văn bản ..... ngày .....

- Có thường xuyên cập nhật công nghệ đảm bảo an toàn thông tin:

□ Có □ Không

2. Về đầu tư

- Đã và dự kiến đầu tư vào các nội dung nào dưới đây:

Nội dung	Năm	Dự kiến năm tiếp theo
Mua thiết bị (phần cứng và phần mềm) an toàn thông tin	□	□
Nghiên cứu sử dụng phần mềm mã nguồn mở	□	□
Đào tạo nguồn nhân lực	□	□
Các nội dung khác:	....	....

- Đã và dự kiến sử dụng những công cụ nào để bảo đảm an toàn thông tin:

Công cụ	Năm	Dự kiến năm tiếp theo
Phần mềm diệt virus	□	□
Mật khẩu	□	□
Tường lửa	□	□
Công cụ mã hóa tập tin	□	□
Chữ ký điện tử	□	□
Mạng riêng ảo VPN	□	□
Hệ thống phát hiện xâm nhập	□	□
Những công cụ khác:	....	....

3. Về tình hình an ninh mạng và xử lý sự cố

- Tổng kết các sự cố an ninh mạng đã xảy ra trong năm:

Sự cố	Số lượng
Virus	
Lừa đảo	
Spyware/Adware	
Tấn công từ chối dịch vụ (Dos, Ddos)	
Nội dung Website đơn vị bị thay đổi (deface website)	
Sự cố khác:	

- Mức độ thiệt hại ước tính trong năm do các sự cố an toàn thông tin gây ra:

□ Thiệt hại gián tiếp: ..... triệu đồng

□ Thiệt hại trực tiếp: ..... triệu đồng

□ Chi phí khắc phục: ..... triệu đồng

- Biện pháp xử lý đã áp dụng khi gặp sự cố:

Phương pháp	Số lần
Không làm gì cả	
Tự xử lý	
Báo cáo cấp trên	
Yêu cầu hỗ trợ từ nơi khác	
Phương pháp khác:	

- Công việc mà cơ quan đã thực hiện sau khi khắc phục được sự cố:

□ Sửa đổi chính sách/hướng dẫn

□ Nâng cao ý thức

□ Đầu tư thêm thiết bị

□ Rà soát lại hệ thống

□ Đào tạo nâng cao cho quản trị

□ Đào tạo nâng cao cho người dùng, ...

4. Tổ chức nhân lực và bồi dưỡng nghiệp vụ:

- Số lượng cán bộ chuyên trách và kiêm nhiệm về công nghệ thông tin:

□ Cán bộ chuyên trách về CNTT, ... người, trình độ chuyên môn: .....

□ Cán bộ kiêm nhiệm về CNTT, ... người, trình độ chuyên môn: .....

- Số lượng cán bộ thực hiện công tác đảm bảo an toàn thông tin trong hoạt động ứng dụng CNTT:

□ Cán bộ thực hiện công tác đảm bảo an toàn thông tin là cán bộ chuyên trách/ kiêm nhiệm về CNTT, ... người, trình độ chuyên môn: .....

□ Cán bộ thực hiện công tác đảm bảo an toàn thông tin không là cán bộ chuyên trách/ kiêm nhiệm về CNTT, ... người, trình độ chuyên môn: .....

- Đơn vị có nhu cầu bồi dưỡng nghiệp vụ an toàn thông tin:

□ Dành cho lãnh đạo và cán bộ quản lý, số lượng dự kiến người

□ Cơ bản/Nâng cao về an toàn thông tin cho cán bộ thực hiện công tác đảm bảo an toàn thông tin, số lượng dự kiến ..... người

□ Cho người dùng, số lượng dự kiến ..... người

II. Ý kiến phản hồi và góp ý thêm

.....

.....

.....

.....

.....

Nơi nhận:
- Sở TT & TT;
- .....

THỦ TRƯỞNG ĐƠN VỊ
(Ký tên và đóng dấu)

PHỤ LỤC 2

MẪU BÁO CÁO SỰ CỐ

(Kèm theo Quyết định số 20 /2017/QĐ-UBND ngày 23 /8/2017 của UBND tỉnh Đắk Nông)

UBND TỈNH ĐẮK NÔNG
TÊN ĐƠN VỊ

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Đắk Nông, ngày tháng năm 20....

BÁO CÁO SỰ CỐ THÁNG/NĂM.....

I. Thông tin chung

1. Tên, địa chỉ Đơn vị vận hành hệ thống thông tin:.....

2. Cơ quan chủ quản hệ thống thông tin:.....

3. E-mail cơ quan: .....

4. Điện thoại cơ quan: .....

II. Thông tin về sự cố an toàn an ninh thông tin

1. Thông tin về sự cố:

- Hệ thống thông tin bị sự cố:.....
- Thời điểm phát hiện sự cố:.....

2. Đầu mối liên lạc về sự cố của đơn vị vận hành hệ thống bị sự cố:

- Họ và tên:.....
- Chức vụ:.....
- Điện thoại:.....; Thư điện tử:.....

3. Mô tả về sự cố:

- Loại sự cố:.....
- Hiện tượng:.....
- Đánh giá sơ bộ mức độ nguy hại; mức độ lây lan; tác động của sự cố đến hoạt động bình thường của tổ chức;

4. Thông tin bổ sung về hệ thống xảy ra sự cố:

-Hệ điều hành..... Version.....

Các dịch vụ có trên hệ thống (*Đánh dấu những dịch vụ được sử dụng trên hệ thống)*

☐ Web server ☐ Mail server ☐ Database server

☐ Dịch vụ khác, đó là.....

Các biện pháp an toàn thông tin đã triển khai (*Đánh dấu những biện pháp đã triển khai)*

☐ Antivirus ☐ Firewall ☐ Hệ thống phát hiện xâm nhập

☐ Khác:.....

Các địa chỉ IP của hệ thống *(Liệt kê địa chỉ IP sử dụng trên Internet, không liệt kê địa chỉ IP nội bộ*..... .

Các tên miền của hệ thống.....

Mục đích chính sử dụng hệ thống .....

Thông tin gửi kèm

☐ Nhật ký hệ thống ☐ Mẫu virus / mã độc ☐ Khác:.....

Các thông tin cung cấp trong thông báo sự cố này đều phải được giữ bí mật: ☐ Có ☐ Không

Sự cố đã được khắc phục: ☐ Đã khắc phục ☐ Chưa khắc phục (đề nghị ứng cứu)

5. Đơn vị cung cấp dịch vụ hạ tầng công nghệ thông tin, viễn thông……

6. Liệt kê các biện pháp đã triển khai hoặc dự kiến triển khai để xử lý khắc phục sự cố:……

7. Các tổ chức, doanh nghiệp đang hỗ trợ ứng cứu, xử lý và kết quả xử lý sự cố tính đến thời điểm báo cáo:……..

8. Kết quả ứng cứu sự cố ban đầu:……..

9. Kiến nghị đề xuất hướng xử lý sự cố (nếu có):……..

THỦ TRƯỞNG ĐƠN VỊ
(Ký tên và đóng dấu)

Nơi nhận:
- Sở TT & TT;
- ...