ỦY BAN NHÂN DÂN TỈNH PHÚ THỌ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 998/QĐ-UBND	*Phú Thọ, ngày 29 tháng 4 năm 2016*

QUYẾT ĐỊNH
Ban hành Quy chế đảm bảo an toàn thông tin mạng trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Phú Thọ

ỦY BAN NHÂN DÂN TỈNH PHÚ THỌ

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

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

Căn cứ Luật Viễn thông ngày 23 tháng 11 năm 2009;

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015 được Quốc hội khóa XIII, kỳ họp thứ 10 thông qua;

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

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;

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

Xét đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Tờ trình số 16/TTr-STTTT ngày 20/4/2016,

QUYẾT ĐỊNH:

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

Điều 2. Quyết định này có hiệu lực kể từ ngày 01/7/2016.

Điều 3. Chánh Văn phòng UBND tỉnh; Giám đốc Sở Thông tin và Truyền thông; Thủ trưởng các sở, ban, ngành; Chủ tịch UBND các huyện, thành, thị; Chủ tịch UBND các xã, phường, thị trấn; các doanh nghiệp viễn thông, công nghệ thông tin trên địa bàn và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Bùi Minh Châu

ỦY BAN NHÂN DÂN
TỈNH PHÚ THỌ

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

QUY CHẾ
Đảm bảo an toàn thông tin mạng trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Phú Thọ

(Ban hành kèm theo Quyết định số: 998/QĐ-UBND ngày 29 tháng 4 năm 2016 của Ủy ban nhân dân tỉnh)

Chương I
NHỮNG QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về công tác đảm bảo an toàn thông tin mạng trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Phú Thọ.

Điều 2. Đối tượng áp dụng

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

2. Các tổ chức, đoàn thể; các doanh nghiệp viễn thông - công nghệ thông tin; người dân, doanh nghiệp và các đơn vị có tham gia vào các hoạt động ứng dụng công nghệ thông tin của tỉnh.

3. Cán bộ, công chức, viên chức và người lao động đang công tác trong các cơ quan, đơn vị nêu tại Khoản 1, Khoản 2 Điều này và những cá nhân, tổ chức có liên quan áp dụng Quy chế này trong việc vận hành, khai thác các hệ thống công nghệ thông tin, hệ thống thông tin tại các cơ quan, đơn vị.

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 hệ thống thông tin và thông tin truyền đưa 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. *Hệ thống thông tin* là tập hợp thiết bị phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin.

4. Trung tâm Dữ liệu số của tỉnh là một công trình xây dựng bao gồm nhà trạm, hệ thống truyền dẫn, hệ thống máy chủ, máy trạm cùng các thiết bị phụ trợ khác để lưu trữ, trao đổi và quản lý tập trung dữ liệu số của tỉnh.

5. Thông tin cá nhân là thông tin gắn với việc xác định danh tính của một người cụ thể.

6. Sự cố an toàn thông tin mạng là việc thông tin, hệ thống thông tin bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.

7. *Rủi ro an toàn thông tin mạng* là những nhân tố chủ quan hoặc khách quan có khả năng ảnh hưởng tới trạng thái an toàn thông tin mạng.

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

Điều 4. Các hành vi bị nghiêm cấm

1. Ngăn chặn, cản trở trái phép việc truy cập, truyền tải thông tin của cơ quan, tổ chức xã hội, doanh nghiệp, cá nhân, gây nguy hại, xóa, làm sai lệch thông tin trên mạng; ảnh hưởng tới hoạt động bình thường của hệ thống thông tin, khả năng truy cập hợp pháp của người sử dụng tới hệ thống thông tin.

2. Tấn công, vô hiệu hóa trái phép làm mất tác dụng của các biện pháp bảo vệ an toàn, an ninh thông tin; tấn công, chiếm quyền điều khiển, thu thập thông tin trái phép đối với hệ thống thông tin.

3. Tạo, cài đặt, phát tán thư rác, tin nhắn rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo.

4. Lợi dụng mạng để truyền bá tư tưởng, văn hóa độc hại, đồi trụy, kích động, chống phá các chủ trương đường lối của Đảng, chính sách pháp luật của Nhà nước.

Điều 5. Các nguyên tắc chung về đảm bảo an toàn thông tin mạng

1. Các văn bản có nội dung mật không được truyền trên mạng mà phải được quản lý theo chế độ mật theo quy định pháp luật hiện hành. Trường hợp đặc biệt, cần truyền thông tin mật trên mạng phải được Thủ trưởng cơ quan, đơn vị cho phép, trước khi truyền thông tin phải được mã hóa theo quy định của Luật Cơ yếu.

2. Các cơ quan, đơn vị phải bố trí máy vi tính riêng, nghiêm cấm sử dụng máy tính kết nối Internet và các thiết bị di động thông minh để soạn thảo văn bản, lưu giữ thông tin có nội dung mật theo quy định. Các thiết bị viễn thông, máy tính được sử dụng để lưu giữ và truyền thông tin bí mật nhà nước phải được chứng nhận của cơ quan chức năng kiểm tra, kiểm định trước khi đưa vào sử dụng.

3. Tổ chức, cá nhân không được xâm phạm an toàn thông tin mạng của tổ chức, cá nhân khác.

4. Phải có phương án tổ chức sao lưu dữ liệu dự phòng cho mọi dữ liệu quan trọng của tỉnh, của cơ quan, đơn vị mình. Lãnh đạo cơ quan, đơn vị phải chịu trách nhiệm nếu để xảy ra mất mát dữ liệu do không tiến hành sao lưu dự phòng.

5. Để phục vụ hoạt động theo dõi, giám sát, phân tích và điều tra, các cơ quan, đơn vị phải thực hiện việc lưu trữ nhật ký của các hệ thống tại các máy chủ (của hệ điều hành và các phần mềm ứng dụng) trong thời gian ít nhất là 30 ngày.

6. Các thiết bị viễn thông, máy tính có chứa tài liệu của cơ quan nhà nước khi đưa đi công tác nước ngoài phải thực hiện theo quy định của pháp luật về bảo vệ bí mật nhà nước.

Chương II
NỘI DUNG ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 6. Đảm bảo an toàn hạ tầng ứng dụng công nghệ thông tin

1. Đảm bảo an toàn thông tin chung cho 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 vào các hệ thống thông tin, trang thiết bị phải có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự số và ký tự đặc biệt như !, @, #, $, %,...) và phải định kỳ thay đổi ít nhất 3 tháng/lần.

c) Tất cả các máy tính tại các cơ quan, đơn vị phải được cài đặt các phần mềm bảo vệ chống virus.

d) Khi xảy ra sự cố lây lan virus tại cơ quan, đơn vị mình phải báo cáo tình hình về Sở Thông tin và Truyền thông.

e) Khi xảy ra sự cố an toàn thông tin mạng thì cơ quan, đơn vị phải có trách nhiệm 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 ngay sự cố.

2. Đảm bảo 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) Tổ chức mô hình mạng nội bộ theo hướng sử dụng máy chủ để quản lý các máy trạm trong mạng, hạn chế sử dụng mô hình mạng ngang hàng (không có máy chủ quản lý).

d) Thiết lập cơ chế bảo vệ mạng nội bộ đảm bảo 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...

e) 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;

f) 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 7. Đảm bảo an toàn dữ liệu, cơ sở dữ liệu và phần mềm ứng dụng công nghệ thông tin

1. Các hệ thống phần mềm, 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 việc di chuyển các trang thiết bị công nghệ thông tin lưu trữ dữ liệu, nhất là các thông tin thuộc danh mục bí mật Nhà nước.

4. Quản lý và phân quyền truy cập phần mềm 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 và thường xuyên cập nhật bản vá lỗ hổng bảo mật từ nhà sản xuất.

6. An toàn khi khai thác, sử dụng các phần mềm dùng chung của tỉnh:

a) Cá nhân khi sử dụng các ứng dụng dùng chung của tỉnh phải ý thức tự bảo vệ thông tin cá nhân của mình; Nghiêm cấm tiết lộ tài khoản đăng nhập, đấu nối, truy cập trái phép vào hệ thống các phần mềm dùng chung của tỉnh.

b) Tài khoản truy cập các phần mềm dùng chung của tỉnh phải đổi mật khẩu mặc định ngay sau khi được Sở Thông tin và Truyền thông cấp, định kỳ thay đổi mật khẩu, đặt mật khẩu với độ an toàn cao; không đặt chế độ ghi nhớ mật khẩu khi sử dụng.

c) Khi khai thác, sử dụng các phần mềm dùng chung của tỉnh tại các điểm truy cập Internet công cộng, tuyệt đối không đặt chế độ lưu trữ 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; cập nhật quyền truy nhập các hệ thống dùng chung, thu hồi các thiết bị CNTT liên quan.

Điều 8. Đảm bảo an toàn thông tin cho Trung tâm Dữ liệu số của tỉnh

1. Xây dựng Quy chế phương án đảm bảo an toàn thông tin mạng cho Trung tâm dữ liệu số của tỉnh; đảm bảo 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 Dữ liệu số của tỉnh phải tuân thủ các chính sách an toàn thông tin liên quan đến việc kết nối vào Trung tâm Dữ liệu số của tỉnh.

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

Điều 9. Phát triển nguồn nhân lực an toàn thông tin mạng

1. Cán bộ chuyên trách về công nghệ thông tin trong các cơ quan đơn vị được bố trí, tạo điều kiện làm việc phù hợp với chuyên môn, được ưu tiên bồi dưỡng nghiệp vụ về an toàn thông tin mạng.

2. Cán bộ chuyên trách về công nghệ thông tin được 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.

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

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 10. Trách nhiệm của các cơ quan, đơn vị

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 Ủy ban nhân dân tỉnh trong công tác đảm bảo an toàn thông tin mạng của cơ quan, đơn vị mình.

2. Bảo vệ an toàn thông tin trong mạng nội bộ là trách nhiệm của các cơ quan, đơn vị quản lý mạng nội bộ đó.

3. Trang bị đầy đủ 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.

4. Bố trí kinh phí cho việc mua sắm, nâng cấp các trang thiết bị phần cứng, phần mềm để đảm bảo và tăng cường an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của cơ quan, đơn vị.

5. Khi có sự cố an toàn thông tin mạng hoặc có nguy cơ mất an toàn thông tin phải kịp thời chỉ đạo khắc phục ngay, ưu tiên sử dụng cán bộ kỹ thuật chuyên trách trong cơ quan, đơn vị, kịp thời 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. 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. Xây dựng quy chế nội bộ về đảm bảo an toàn thông tin trong cơ quan, đơn vị mình.

7. 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 cho hệ thống công nghệ thông tin và các hệ thống thông tin của cơ quan, đơn vị mình.

8. 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.

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; đồng thời cung cấp đầy đủ các thông tin khi đoàn kiểm tra yêu cầu. Không được che dấu thông tin về sự cố nhằm gây khó khăn cho các cơ quan chức năng đánh giá thiệt hại để có phương án xử lý.

10. Báo cáo tình hình và kết quả thực hiện công tác đảm bảo an toàn thông tin tại cơ quan, đơn vị, định kỳ hàng năm (trước ngày 15/11) gửi về Sở Thông tin và Truyền thông.

Điều 11. Trách nhiệm của Sở Thông tin và Truyền thông

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

2. Là cơ quan đầu mối về ứng cứu sự cố máy tính của tỉnh, tham gia vào mạng lưới điều phối ứng cứu sự cố Internet và là đầu mối về tiếp nhận và xử lý các vấn đề liên quan đến thư rác, tin nhắn rác.

3. Chịu trách nhiệm xây dựng và trình Ủy ban 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.

4. Tham mưu Ủy ban nhân dân tỉnh hướng dẫn việc sử dụng các thiết bị Công nghệ thông tin để lưu giữ và truyền tải thông tin bí mật nhà nước.

5. Nghiên cứu, 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 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.

6. Chủ trì hoạt động kiểm tra đánh giá công tác đảm bảo an toàn thông tin trong các cơ quan, đơn vị trong tỉnh và thực hiện đánh giá an toàn thông tin cho các hệ thống thông tin trong cơ quan, đơn vị mình quản lý.

7. 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 công nghệ thông tin của cơ quan nhà nước.

8. 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.

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. Là đầu mối của tỉnh, phối hợp với Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT), các cơ quan, đơn vị có liên quan xử lý, ứng cứu các sự cố mất an toàn thông tin trên địa bàn tỉnh. Hướng dẫn cụ thể về nghiệp vụ quản lý vận hành, kỹ thuật đảm bảo 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. Thiết lập đường dây nóng, bố trí cán bộ thường trực để tiếp nhận các phản ánh của các cơ quan, đơn vị về nguy cơ gây mất an toàn thông tin; phối hợp hướng dẫn, xử lý kịp thời.

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.

Điều 12. Trách nhiệm của Công an tỉnh

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

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

3. Thường xuyên thông báo cho các cơ quan, đơn vị về phương thức, thủ đoạn của các loại tội phạm xâm phạm an toàn thông tin để có biện pháp phòng ngừa, phát hiện, đấu tranh, ngăn chặn.

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

Điều 13. Trách nhiệm của Sở Tài chính, Sở Kế hoạch và Đầu tư

Phối hợp cùng Sở Thông tin và Truyền thông tham mưu UBND tỉnh bố trí kinh phí cho các hoạt động đảm bảo an toàn thông tin mạng trong hoạt động của các cơ quan nhà nước trên địa bản tỉnh.

Điều 14. Trách nhiệm của các tổ chức, đoàn thể; các doanh nghiệp viễn thông, công nghệ thông tin tham gia vào các hệ thống mạng ứng dụng công nghệ thông tin của tỉnh

1. Các tổ chức, đoàn thể: Chịu trách nhiệm triển khai thực hiện các biện pháp đảm bảo an toàn thông tin theo quy định tại Điều 10 Quy chế này.

2. Các doanh nghiệp viễn thông, công nghệ thông tin cung cấp hạ tầng phục vụ ứng dụng công nghệ thông tin trong cơ quan nhà nước:

a) Các doanh nghiệp viễn thông có trách nhiệm đầu tư, phát triển hạ tầng viễn thông, đường truyền phục vụ việc ứng dụng công nghệ thông tin đảm bảo an toàn thông tin cho hệ thống do doanh nghiệp thiết lập.

b) Viễn thông Phú Thọ có trách nhiệm đảm bảo hệ thống mạng truyền số liệu chuyên dùng của cơ quan Đảng, Nhà nước; phối hợp với Bưu điện Trung ương, Sở Thông tin và Truyền thông trong việc xử lý khắc phục sự số mạng truyền số liệu chuyên dùng của cơ quan Đảng, Nhà nước.

Điều 15. Trách nhiệm của 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 của đơn vị.

b) Chịu trách nhiệm triển khai các biện pháp quản lý, vận hành, quản lý kỹ thuật, tham mưu xây dựng quy định về đảm bảo an toàn cho hệ thống thông tin của cơ quan, đơn vị theo Quy chế này.

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

d) Tham gia các đầy đủ các khóa đào tạo về đảm bảo an toàn thông tin mạng do UBND tỉnh tổ chức.

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

a) Chấp hành nghiêm túc các quy định về an toàn thông tin của cơ quan, đơn vị cũng như các quy định khác của pháp luật, nâng cao ý thức cảnh giác và trách nhiệm đảm bảo an toàn thông tin tại cơ quan, đơn vị.

b) Mỗi cán bộ, công chức, viên chức và người lao động phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; Chịu trách nhiệm thông tin cá nhân khai báo, không tiết lộ tài khoản, mật khẩu các ứng dụng dùng chung của tỉnh khi được cấp.

b) Khi phát hiện sự cố mất an toàn thông tin phải báo ngay với cấp trên và bộ phận chuyên trách của cơ quan, đơn vị để kịp thời ngăn chặn, xử lý.

c) Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng do UBND tỉnh, Sở Thông tin và Truyền thông hoặc các cơ quan, đơn vị chuyên môn tổ chức.

Điều16. Trách nhiệm của người dân, doanh nghiệp khi tương tác các hệ thống ứng dụng công nghệ thông tin phục vụ giao tiếp

1. Tuân thủ theo quy định tại Quy chế này và các quy định khác của pháp luật có liên quan.

2. Thực hiện tốt các biện pháp đảm bảo an toàn thông tin khi tương tác sử dụng ứng dụng công nghệ thông tin phục vụ người dân và doanh nghiệp.

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

4. 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 công nghệ thông tin thông tin để thu thập, khai thác thông tin cá nhân.

Chương IV
CÔNG TÁC THANH TRA, KIỂM TRA AN TOÀN THÔNG TIN MẠNG

Điều 17. Kế hoạch thanh tra, kiểm tra hàng năm

1. Sở Thông tin và Truyền thông chủ trì, phối hợp Công an tỉnh và các cơ quan, đơn vị có liên quan định kỳ hàng năm tiến hành công tác thanh tra, kiểm tra, xử lý các hành vi vi phạm an toàn thông tin mạng tại các cơ quan nhà nước trên địa bàn tỉnh.

2. Kiểm tra đột xuất các cơ quan, đơn vị khi có dấu hiệu vi phạm an toàn thông tin mạng.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 18. Khen thưởng và xử lý vi phạm

1. Hàng năm, Sở Thông tin và Truyền thông dựa trên các điều tra, báo cáo công tác an toàn thông tin của các cơ quan, đơn vị đưa an toàn thông tin mạng vào tiêu chí đánh giá xếp hạng ứng dụng CNTT của các cơ quan nhà nước trên địa bàn tỉnh, trên cơ sở đó đề xuất UBND tỉnh xem xét khen thưởng theo quy định.

2. Các cơ quan, đơn vị; cá nhân ; Người dân và doanh nghiệp khi vi phạm quy định của Quy chế này, tùy theo tính chất, mức độ vi phạm mà bị xử phạt vi phạm hành chính hoặc bị truy cứu trách nhiệm hình sự, nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật.

Điều 19. Điều khoản thi hành

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 UBND tỉnh xem xét sửa đổi, bổ sung Quy chế cho phù hợp./.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Bùi Minh Châu