UỶ BAN NHÂN DÂN **TỈNH TUYÊN QUANG**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 17 /2014/QĐ-UBND	*Tuyên Quang, ngày 21 tháng 10 năm 2014*

QUYẾT ĐỊNH

Ban hành Quy chế Đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước tỉnh Tuyên Quang

UỶ BAN NHÂN DÂN TỈNH TUYÊN QUANG

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

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

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

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

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

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

Căn cứ Chỉ thị số 15/CT-TTg ngày 17 tháng 6 năm 2014 của Thủ tướng Chính phủ về tăng cường công tác đảm bảo an ninh và an toàn thông tin mạng trong tình hình mới;

Theo đề nghị của Sở Thông tin và Truyền thông tại Tờ trình số 36/TTr-STTTT ngày 18/8/2014 về việc ban hành Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước tỉnh Tuyên Quang,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước tỉnh Tuyên Quang.

Điều 2. Giao Sở Thông tin và Truyền thông hướng dẫn, kiểm tra đôn đốc các sở, ban, ngành, Ủy ban nhân dân huyện, thành phố và các cơ quan có liên quan thực hiện Quyết định này.

Điều 3. Quyết định này có hiệu lực thi hành kể từ ngày 01/11/2014.

Chánh Văn phòng Ủy ban nhân dân tỉnh; Giám đốc Sở Thông tin và Truyền thông, Giám đốc các sở; thủ trưởng các ban, ngành thuộc tỉnh; Chủ tịch Ủy ban nhân dân các huyện, thành phố; các cơ quan, đơn vị và tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành quyết định này./.

TM. UỶ BAN NHÂN DÂN
CHỦ TỊCH

Chẩu Văn Lâm

Nơi nhận:
- Văn phòng Chính phủ;
- Bộ Thông tin và Truyền thông; (Báo cáo)
- TT Tỉnh uỷ;
- TTHĐND tỉnh;
- Cục kiểm tra VBQPPL - Bộ Tư pháp;
- Đoàn đại biểu Quốc hội tỉnh;
- Chủ tịch UBND tỉnh;
- Phó Chủ tịch UBND tỉnh;
- Uỷ ban MTTQ và các đoàn thể tỉnh;
- Các ban Đảng, Văn phòng Tỉnh ủy;
- Công báo Tuyên Quang;
- Như Điều 3;
- CVP, PCVP UBND tỉnh;
- Lưu: VT.

UỶ BAN NHÂN DÂN **TỈNH TUYÊN QUANG**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**

QUY CHẾ

Đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước tỉnh Tuyên Quang

(Ban hành kèm theo Quyết định số 17 /2014/QĐ-UBND, ngày 21/10/2014 của Uỷ ban nhân dân tỉnh Tuyên Quang)

Chương I

QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về công tác đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng, phát triển công nghệ thông tin của cơ quan nhà nước; trách nhiệm của cơ quan nhà nước trong việc thực hiện các biện pháp nhằm đảm bảo an toàn, an ninh thông tin trên địa bàn tỉnh Tuyên Quang.

Điều 2. Đối tượng áp dụng

1. Quy chế này được áp dụng đối với các cơ quan quản lý hành chính nhà nước và các đơn vị sự nghiệp trên địa bàn tỉnh Tuyên Quang (*sau đây gọi tắt là các cơ quan, đơn vị*).

2. Các cán bộ, công chức, viên chức đang làm việc trong các cơ quan, đơn vị nêu tại khoản 1 Điều này áp dụng Quy định này trong việc vận hành, khai thác và sử dụng hệ thống thông tin tại các cơ quan, đơn vị.

Điều 3. Nguyên tác áp dụng

Những vấn đề không quy định tại Quy chế này thì thực hiện theo quy định của Luật Công nghệ thông tin; Nghị định số 64/2007/NĐ-CP của Chính phủ và các văn bản pháp luật có liên quan.

Điều 4. Giải thích từ ngữ

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

1. *Cấu hình chuẩn:* Là cấu hình được các nhà sản xuất thiết bị, phần mềm, khuyến nghị áp dụng, nhằm loại bỏ các xung đột, lỗ hổng có thể xảy ra trong quá trình cấu hình thiết bị.

2. *Cổng giao tiếp (Port)*: Để định danh các ứng dụng gửi và nhận dữ liệu, mỗi ứng dụng sẽ tương ứng với một cổng giao tiếp, những ứng dụng phổ biến được đặt với số hiệu cổng định trước, nhằm định danh duy nhất các ứng dụng đó. Khi máy tính sử dụng dịch vụ nào thì cổng giao tiếp tương ứng với dịch vụ đó sẽ mở.

3. *Giao thức*: Là tập hợp các quy tắc, quy ước truyền thông của mạng mà tất cả các thực thể tham gia truyền thông phải tuân theo.

4. *Bản ghi nhật ký hệ thống (Logfile)*: Là một tập tin được tạo ra trên mỗi thiết bị của hệ thống thông tin như tường lửa, máy chủ ứng dụng,... có chứa tất cả thông tin về các hoạt động xảy ra trên thiết bị đó. Bản ghi nhật ký hệ thống dùng để phân tích những sự kiện đã xảy ra, nguồn gốc và các kết quả để có các biện pháp xử lý thích hợp.

5. *Mạng ngang hàng*: Là mạng mà trong đó các máy tính có quyền bình đẳng như nhau, mỗi máy tính có quyền chia sẻ tài nguyên và sử dụng các tài nguyên từ máy tính khác.

Chương II

NỘI DUNG ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 5. Các biện pháp chung đảm bảo an toàn, an ninh thông tin

1. Đối với các cơ quan, đơn vị:

a) Trang bị đầy đủ các kiến thức bảo mật cơ bản cho cán bộ, công chức, viên chức trước khi cho phép truy nhập và sử dụng hệ thống thông tin;

b) Bố trí cán bộ, công chức, viên chức phụ trách về an toàn hệ thống thông tin (*sau đây gọi tắt là cán bộ phụ trách*). Cán bộ phụ trách được đảm bảo điều kiện học tập, tiếp cận công nghệ, kiến thức an toàn bảo mật thông tin trước khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ;

c) Xác định và phân bổ kinh phí cho các hoạt động liên quan đến việc bảo vệ hệ thống thông tin, thông qua việc đầu tư các thiết bị tường lửa, các chương trình chống thư rác, virus máy tính trên các máy trạm, máy chủ,...và các công việc khác có liên quan đến việc bảo đảm an toàn, an ninh thông tin;

d) Các cơ quan, đơn vị phải bố trí ít nhất 01 máy vi tính riêng, không kết nối mạng nội bộ và Internet dùng để quản lý, lưu giữ, soạn thảo các tài liệu mật theo quy định. Nghiêm cấm lưu trữ, trao đổi, xử lý, hiển thị thông tin, tài liệu có nội dung bí mật nhà nước, bí mật nội bộ trên mạng viễn thông, Internet không có biện pháp bảo mật theo quy định; kết nối máy tính, thiết bị điện tử có chứa thông tin bí mật nhà nước, bí mật nội bộ vào mạng Internet;

đ) Kiểm tra việc thực hiện các nội dung của Điều 6 Quy chế này.

2. Đối với cán bộ phụ trách tại các cơ quan đơn vị:

a) Triển khai, thực hiện các nội dung của Điều 6 Quy chế này;

b) Tham mưu về các biện pháp bảo đảm an toàn thông tin; vận hành an toàn hệ thống thông tin của đơn vị, triển khai các biện pháp bảo đảm an toàn, an ninh thông tin cho tất cả cán bộ, công chức, viên chức trong đơn vị mình;

c) Thường xuyên cập nhật cấu hình chuẩn cho các thành phần của hệ thống thông tin, thiết lập cấu hình chặt chẽ nhất cho các sản phẩm an toàn thông tin nhưng vẫn duy trì yêu cầu hoạt động của hệ thống thông tin;

d) Khi thực hiện việc cấu hình hệ thống thông tin chỉ cung cấp những chức năng thiết yếu nhất; xác định các chức năng, cổng giao tiếp mạng, giao thức, và dịch vụ không cần thiết để cấm hoặc hạn chế sử dụng;

đ) Thường xuyên thực hiện việc theo dõi bản ghi nhật ký hệ thống (*logfile*) 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;

e) Kiểm soát chặt chẽ việc cài đặt phần mềm vào máy trạm và máy chủ.

3. Đối với cán bộ, công chức, viên chức:

a) Thường xuyên cập nhật chính sách, thủ tục an toàn thông tin của đơn vị và thực hiện hướng dẫn về an toàn, an ninh thông tin của cán bộ phụ trách;

b) Hạn chế việc sử dụng chức năng chia sẻ tài nguyên (*sharing*), nếu sử dụng chức năng này cần bật thuộc tính bảo mật bằng mật khẩu và thực hiện việc thu hồi chức năng này khi đã sử dụng xong;

c) Các máy tính khi không sử dụng trong thời gian dài (*quá 02 giờ làm việc*) cần tắt máy hoặc ngưng kết nối mạng (*trừ hệ thống máy chủ*);

d) Khi mở các tập tin đính kèm theo thư điện tử, nếu biết rõ người gửi thư thì phải lưu tập tin vào máy tính rồi quét virus trước khi mở, không được mở các thư điện tử có tập tin đính kèm có nguồn gốc không rõ ràng để phòng, tránh virus, phần mềm gián điệp đính kèm theo thư;

đ) Phải đặt mật khẩu truy nhập vào máy tính của mình, đồng thời thiết lập chế độ bảo vệ màn hình (*screen saver*) có sử dụng mật khẩu bảo vệ sau một khoảng thời gian nhất định không sử dụng máy tính. Khi gắn thiết bị lưu trữ vào máy tính, không được trực tiếp truy cập ngay mà phải quét virus trước;

e) Khi đặt các loại mật khẩu (*tệp tin, máy tính, thư điện tử, tài khoản phần mềm quản lý văn bản,...*) nên nhiều hơn 8 ký tự, có cả số và chữ; đồng thời các loại mật khẩu nên thay đổi sau một khoảng thời gian đưa vào sử dụng (*khoảng sau 01 tháng*), nếu có dấu hiệu lộ phải thay đổi ngay.

Điều 6. Các biện pháp kỹ thuật đảm bảo an toàn, an ninh thông tin

1. Tổ chức mô hình mạng:

a) Cài đặt, cấu hình, tổ chức hệ thống mạng theo mô hình Clients/Server, hạn chế sử dụng mô hình mạng ngang hàng. Đối với các cơ quan, đơn vị có nhiều phòng, ban, đơn vị trực thuộc không nằm trong cùng một khu vực thì cần thiết lập mạng riêng ảo (*VPN*) để tăng cường an ninh cho hạ tầng mạng nội bộ;

b) Khi thiết lập các dịch vụ trên môi trường mạng Internet, chỉ cung cấp những chức năng thiết yếu nhất bảo đảm duy trì hoạt động của hệ thống thông tin; hạn chế sử dụng chức năng, cổng giao tiếp mạng, giao thức và các dịch vụ không cần thiết.

2. Quản lý hệ thống mạng không dây: Khi thiết lập mạng không dây để kết nối với mạng cục bộ thông qua các điểm truy nhập (*Access Point -AP*), cần thiết lập các tham số như: tên, mật khẩu, mã hóa dữ liệu và thông báo các thông tin liên quan đến AP để cơ quan sử dụng, định kỳ 3 tháng thay đổi mật khẩu nhằm tăng cường công tác bảo mật.

3. Tổ chức quản lý tài khoản của các hệ thống thông tin, bao gồm: Tạo mới, kích hoạt, sửa đổi, vô hiệu hóa và loại bỏ các tài khoản. Thường xuyên kiểm tra các tài khoản của hệ thống thông tin và triển khai các công cụ tự động để hỗ trợ việc quản lý các tài khoản của hệ thống. Hủy tài khoản, quyền truy nhập hệ thống thông tin, thu hồi lại tất cả các tài sản liên quan tới hệ thống thông tin (*khóa, thẻ nhận dạng, thư mục lưu trữ,...*) đối với cán bộ, công chức, viên chức, nhân viên đã chuyển công tác hoặc chấm dứt hợp đồng lao động nhưng vẫn đảm bảo khả năng truy cập vào các hồ sơ được tạo ra bởi cán bộ, công chức, viên chức hoặc nhân viên đó.

4. Quản lý đăng nhập hệ thống: Các hệ thống thông tin cần giới hạn một số hữu hạn lần đăng nhập sai liên tiếp. Hệ thống tự động khóa tài khoản hoặc cô lập tài khoản trong một khoảng thời gian nhất định trước khi tiếp tục cho đăng nhập nếu liên tục đăng nhập sai vượt quá số lần quy định. Tổ chức theo dõi, và kiểm soát tất cả các phương pháp truy nhập từ xa (*quay số, Internet...*) tới hệ thống thông tin, tăng cường việc sử dụng mạng riêng ảo (*VPN - Virtual Private Network*) khi có nhu cầu làm việc từ xa.

5. Quản lý Logfile: Hệ thống thông tin cần ghi nhận được các sự kiện cần thiết phục vụ quá trình kiểm soát: quá trình đăng nhập hệ thống, các thao tác cấu hình hệ thống, quá trình truy xuất hệ thống, ghi nhận đầy đủ các thông tin trong các bản ghi nhật ký để xác định những sự kiện nào đã xảy ra, nguồn gốc và các kết quả của sự kiện để có cơ chế bảo vệ và lưu giữ nhật ký trong một khoảng thời gian nhất định.

6. Chống mã độc, virus: Lựa chọn, triển khai các phần mềm phòng chống virus, thư rác trên các máy trạm, máy chủ, các thiết bị di động trong mạng và những hệ thống thông tin xung yếu như: Cổng/trang thông tin điện tử, thư điện tử, một cửa điện tử,... để phát hiện, loại trừ những đoạn mã độc hại. Thường xuyên cập nhật các phiên bản mới, các bản vá lỗi của các phần mềm chống virus, thiết lập chế độ quét tự động thường xuyên ít nhất là hằng tuần.

7. Tổ chức quản lý tài nguyên: Kiểm tra, giám sát chức năng chia sẻ thông tin (*Network File and Folder Sharing*); khuyến cáo người sử dụng cân nhắc việc chia sẻ tài nguyên cục bộ trên máy đang sử dụng. Khi thực hiện việc chia sẻ tài nguyên trên máy chủ hoặc trên máy cục bộ phải sử dụng mật khẩu để bảo vệ thông tin.

8. Thiết lập cơ chế sao lưu và phục hồi hệ thống:

Hệ thống thông tin phải có cơ chế sao lưu thông tin ở mức người dùng và mức hệ thống, các thông tin sao lưu phải lưu trữ tại nơi an toàn; đồng thời thường xuyên kiểm tra để đảm bảo khả năng phục hồi hệ thống khi có sự cố xảy ra.

9. Xử lý khẩn cấp: Khi phát hiện hệ thống bị tấn công, thông qua các dấu hiệu như luồng tin tăng lên bất ngờ, nội dung trang chủ Web bị thay đổi, hệ thống hoạt động rất chậm khác thường,... cần thực hiện các bước cơ bản sau:

a) Bước 1: Ngắt kết nối máy chủ ra khỏi mạng;

b) Bước 2: Sao chép logfile và toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ (*phục vụ cho công tác phân tích*);

c) Bước 3: Khôi phục hệ thống bằng cách sử dụng dữ liệu backup mới nhất để hệ thống hoạt động;

d) Bước 4: Thực hiện các công việc được quy định tại khoản 2 Điều 9.

10. Hệ thống thông tin cần có cơ chế ngăn chặn hoặc hạn chế các sự cố gây ra do tấn công từ chối dịch vụ (*DoS, DDoS*). Đối với hệ thống thông tin cho phép truy nhập công cộng thì có thể được bảo vệ bằng cách tăng dung lượng, băng thông hoặc thiết lập hệ thống dự phòng.

Điều 7. Xây dựng quy chế nội bộ đảm bảo an toàn, an ninh thông tin

Các cơ quan, đơn vị phải ban hành quy chế nội bộ, đảm bảo quy định rõ các vấn đề sau:

1. Mục tiêu và phương hướng thực hiện công tác đảm bảo an toàn an ninh cho hệ thống thông tin.

2. Nguyên tắc phân loại và quản lý mức độ ưu tiên đối với các tài nguyên của hệ thống thông tin (*phần mềm, dữ liệu, trang thiết bị...*).

3. Quản lý phân quyền và trách nhiệm đối với từng cá nhân khi tham gia sử dụng hệ thống thông tin.

4. Quản lý và điều hành hệ thống máy chủ, thiết bị mạng, thiết bị bảo vệ mạng một cách an toàn.

5. Kiểm tra, rà soát và khắc phục sự cố an toàn an ninh của hệ thống thông tin sử dụng các biện pháp trong Điều 5 và Điều 6 Quy chế này.

6. Báo cáo tổng hợp tình hình an toàn, an ninh của hệ thống thông tin theo định kỳ.

7. Các biện pháp tổ chức thực hiện.

Chương III

TRÁCH NHIỆM ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 8. Sở Thông tin và Truyền thông

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

2. Hàng năm xây dựng kế hoạch, dự toán nguồn kinh phí để triển khai công tác an toàn và an ninh thông tin phục vụ cho việc vận hành các hệ thống thông tin được Ủy ban nhân dân tỉnh giao quản lý.

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

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

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

6. Chủ trì, phối hợp với Công an tỉnh và các đơn vị có liên quan tiến hành thanh tra, kiểm tra công tác đảm bảo an toàn, an ninh thông tin đối với các cơ quan nhà nước cấp tỉnh, Ủy ban nhân dân các huyện, thành phố.

7. Xử lý theo thẩm quyền các hành vi vi phạm an toàn, an ninh thông tin gây thiệt hại cho hệ thống thông tin các cơ quan Nhà nước trên địa bàn tỉnh.

Điều 9. Các cơ quan, đơn vị

1. Thủ trưởng các cơ quan, đơn vị có trách nhiệm tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm toàn diện trước Ủy ban nhân dân tỉnh trong công tác bảo vệ an toàn, an ninh thông tin của cơ quan, đơn vị mình.

2. Khi có sự cố hoặc nguy cơ mất an toàn thông tin phải kịp thời áp dụng mọi biện pháp để khắc phục và hạn chế thiệt hại, ưu tiên sử dụng lực lượng kỹ thuật an toàn, an ninh thông tin của đơn vị và lập biên bản, báo cáo bằng văn bản cho cơ quan cấp trên quản lý trực tiếp và Sở Thông tin và Truyền thông. Trường hợp có sự cố nghiêm trọng vượt quá khả năng khắc phục của đơn vị, phải báo cáo ngay cho cơ quan cấp trên quản lý trực tiếp và Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ.

3. Cử cán bộ phụ trách tham gia Đoàn kiểm tra, đánh giá công tác an toàn, an ninh thông tin khi có yêu cầu từ Sở Thông tin và Truyền thông. Phối hợp xây dựng các tiêu chí và quy trình kỹ thuật kiểm tra công tác an toàn, an ninh thông tin.

4. 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, an ninh thông tin. Tạo điều kiện thuận lợi cho các cơ quan chức năng tham gia khắc phục sự cố và thực hiện đúng theo hướng dẫn.

5. Phối hợp với đoàn kiểm tra để triển khai công tác kiểm tra khắc phục sự cố diễn ra nhanh chóng và đạt hiệu quả; đồng thời cung cấp đầy đủ các thông tin khi đoàn kiểm tra yêu cầu.

6. Thường xuyên thông báo cho 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.

7. Báo cáo tình hình và kết quả thực hiện công tác đảm bảo an toàn, an ninh thông tin tại cơ quan, đơn vị và gửi về Sở Thông tin và Truyền thông định kỳ hàng năm (*trước ngày 20 tháng 01*).

Điều 10. Cán bộ, công chức, viên chức

1. Cán bộ phụ trách

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

b) 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.

2. Cán bộ, công chức, viên chức trong các cơ quan, đơn vị

a) Nghiêm chỉnh thi hành các quy chế nội bộ, quy trình về an toàn, an ninh 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 ninh thông tin tại đơn vị.

b) Khi phát hiện sự cố phải báo cáo ngay với cấp trên và bộ phận phụ trách, đồng thời cung cấp các thông tin để kịp thời ngăn chặn, xử lý.

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

Điều 11. Công an tỉnh

1. Phối hợp Sở Thông tin và Truyền thông kiểm tra công tác an toàn, an ninh thông tin;

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

Chương IV

TỔ CHỨC THỰC HIỆN

Điều 12. 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, an ninh thông tin của các cơ quan, đơn vị đề xuất với Ủy ban nhân dân tỉnh xét khen thưởng cho các cá nhân, đơn vị có thành tích đảm bảo an toàn, an ninh thông tin theo quy định hiện hành.

2. Tổ chức, cá nhân có hành vi vi phạm các quy định về an toàn, an ninh thông tin trong ứng dụng công nghệ thông tin của cơ quan Nhà nước, tùy theo tính chất, mức độ vi phạm sẽ bị xử phạt vi phạm hành chính hoặc truy cứu trách nhiệm hình sự theo quy định của pháp luật.

Điều 13. Điều khoản thi hành

Sở Thông tin và Truyền thông chủ trì, phối hợp với các sở, ban, ngành, Ủy ban nhân dân huyện, thành phố và các cơ quan có liên quan triển khai thực hiện Quy chế này.

Trong quá trình thực hiện, nếu có khó khăn, vướng mắc cần điều chỉnh, sửa đổi, bổ sung, đề nghị các cơ quan, đơn vị, địa phương báo cáo bằng văn bản về Sở Thông tin và Truyền thông để tổng hợp, báo cáo Ủy ban nhân dân tỉnh xem xét, điều chỉnh cho phù hợp./.

TM. UỶ BAN NHÂN DÂN
CHỦ TỊCH

Chẩu Văn Lâm