ỦY BAN NHÂN DÂN TỈNH CAO BẰNG	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 50 /2014/QĐ-UBND	*Cao Bằng, ngày 19 tháng 12 năm 2014*

QUYẾT ĐỊNH

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

ỦY BAN NHÂN DÂN TỈNH CAO BẰNG

Căn cứ Luật Tổ chức Hội đồng nhân dân và Ủy 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 tỉnh, Ủy ban nhân dân tỉnh 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 06 năm 2006;

Căn cứ Nghị định 64/2007/NĐ-CP ngày 10 tháng 04 năm 2007 của Chính phủ về việc Ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

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

Căn cứ Thông tư số 23/2011/TT-BTTTT ngày 11 tháng 8 năm 2011 của Bộ Thông tin và Truyền thông quy định về việc quản lý, vận hành, sử dụng và bảo đảm an toàn thông tin trên mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước;

Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Tờ trình số 301/TTr-STTTT ngày 01 tháng 12 năm 2014,

QUYẾT ĐỊNH:

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

Điều 2. Quyết định này có hiệu lực thi hành sau 10 ngày kể từ ngày ký ban hành.

Điều 3. Chánh Văn phòng Ủy ban nhân dân tỉnh; Giám đốc Sở Thông tin và Truyền thông; Thủ trưởng các cơ quan, đơn vị; Chủ tịch Ủy ban nhân dân các huyện, thành phố và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Bộ Thông tin và Truyền thông;
- Cục kiểm tra văn bản QPPL- Bộ Tư pháp;
- Thường trực Tỉnh ủy;
- Thường trực HĐND tỉnh;
- Chủ tịch, các Phó Chủ tịch UBND tỉnh;
- Các cơ quan đoàn thể tỉnh;
- Các PCVP UBND tỉnh;
- Trung tâm thông tin, VPUBND tỉnh;
- Lưu: VT, VX (G).

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Nguyễn Hoàng Anh

ỦY BAN NHÂN DÂN
TỈNH CAO BẰNG

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

QUY CHẾ

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

(Ban hành kèm theo Quyết định số: 50 /2014/QĐ-UBND ngày 19 tháng 12 năm 2014 của Ủy ban nhân dân tỉnh Cao Bằng)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về công tác đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin (CNTT) của các cơ quan nhà nước trên địa bàn tỉnh Cao Bằng.

Điều 2. Đối tượng áp dụng

Quy chế này áp dụng đối với cơ quan nhà nước của tỉnh Cao Bằng bao gồm các sở, ban, ngành trực thuộc Ủy ban nhân dân tỉnh, Ủy ban nhân dân cấp huyện, Ủy ban nhân dân cấp xã. Khuyến khích các cơ quan đảng, đoàn thể, tổ chức Chính trị - Xã hội áp dụng Quy chế này trong hoạt động ứng dụng CNTT.

Điều 3. Giải thích từ ngữ

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

1. Ứng dụng CNTT là việc sử dụng CNTT vào các hoạt động thuộc lĩnh vực kinh tế - xã hội, đối ngoại, quốc phòng, an ninh và các hoạt động khác nhằm nâng cao năng suất, chất lượng, hiệu quả của các hoạt động này.

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

3. An ninh thông tin là việc bảo đảm thông tin trên mạng không gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân

4. Hệ thống thông tin là tập hợp các thiết bị viễn thông, công nghệ

thông tin bao gồm phần cứng, phần mềm và cơ sở dữ liệu phục vụ cho hoạt động lưu trữ, xử lý, truyền đưa, chia sẻ, trao đổi, cung cấp và sử dụng thông tin.

5. Quản lý rủi ro an toàn thông tin là việc thực hiện đánh giá rủi ro an toàn thông tin, xác định yêu cầu bảo vệ thông tin và hệ thống thông tin và áp dụng giải pháp phòng, chống, giảm thiểu thiệt hại khi có sự cố mất an toàn thông tin.

6. Đánh giá rủi ro an toàn thông tin là việc xác định, phân tích nguy cơ mất an toàn thông tin có thể có và dự báo mức độ, phạm vi ảnh hưởng và khả năng gây thiệt hại khi xảy ra sự cố mất an toàn thông tin.

7. Mô hình Clients/Server là mô hình sử dụng máy chủ để cung cấp dịch vụ, xử lý các yêu cầu gửi từ máy trạm.

8. Mạng riêng ảo (Virtual Private Network - VPN) là mạng dành riêng để kết nối các máy tính với nhau thông qua mạng Internet.

9. Tường lửa (firewall) là một thuật ngữ dùng mô tả những thiết bị hay phần mềm có nhiệm vụ lọc những thông tin đi vào hay đi ra một hệ thống mạng hay máy tính theo những quy định đã được thiết lập trước đó.

10. Thiết bị định tuyến (router) là một thiết bị mạng máy tính dùng để chuyển các gói dữ liệu qua một liên mạng và đến các đầu cuối, thông qua một tiến trình được gọi là định tuyến.

11. Phần mềm độc hại (mã độc) 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.

12. 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.

13. 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.

Điều 4. Mục đích, nguyên tắc đảm bảo an toàn thông tin

1. Việc áp dụng Quy chế này nhằm giảm thiểu các nguy cơ gây mất an toàn thông tin và đảm bảo an ninh thông tin trong quá trình ứng dụng CNTT trong hoạt động của các cơ quan.

2. Các hoạt động ứng dụng CNTT phải tuân theo nguyên tắc đảm bảo an toàn thông tin được quy định tại Điều 41, Nghị định 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ về ứng dụng CNTT trong hoạt động của cơ quan nhà nước.

Điều 5. Các hành vi bị nghiêm cấm

1. Tạo ra, cài đặt, phát tán virus máy tính, phần mềm độc hại trái pháp luật.

2. Xâm nhập, sửa đổi, xóa bỏ nội dung thông tin của cơ quan, cá nhân khác khi chưa được sự cho phép.

3. Cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin

4. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của cơ quan, cá nhân khác trên môi trường mạng.

5. Hành vi khác làm mất an toàn, bí mật thông tin của cơ quan, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

Chương II
QUY ĐỊNH ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 6. Nội dung bảo vệ hệ thống thông tin

1. Ban hành quy định về bảo đảm an toàn thông tin trong thiết kế, xây dựng, quản lý, vận hành, sử dụng, nâng cấp, hủy bỏ hệ thống thông tin.

2. Áp dụng biện pháp quản lý và kỹ thuật phù hợp với tiêu chuẩn, quy chuẩn kỹ thuật hiện có về an toàn thông tin để phòng, chống nguy cơ, khắc phục sự cố an toàn thông tin.

3. Kiểm tra, giám sát việc tuân thủ quy định và đánh giá hiệu quả của các biện pháp quản lý và kỹ thuật được áp dụng.

4. Quản lý rủi ro an toàn thông tin (nhằm phân tích những gì có thể xảy ra và hậu quả có thể gặp phải, trước khi quyết định thực hiện để giảm rủi ro tới mức chấp nhận được).

Điều 7. Về quản lý cán bộ, công chức, viên chức

1. Các cơ quan, đơn vị phải thường xuyên tổ chức quán triệt các quy định về an toàn thông tin, nhằm nâng cao nhận thức về trách nhiệm đảm bảo an toàn thông tin của từng cá nhân trong cơ quan.

2. Hủy tài khoản, quyền truy cập các hệ thống thông tin, thu hồi lại tất cả các tài sản liên quan tới hệ thống thông tin của cơ quan (tài khoản, máy vi tính, thiết bị lưu trữ, ...) đối với các cá nhân nghỉ việc, chuyển công tác.

Điều 8. Các biện pháp quản lý kỹ thuật cho công tác đảm bảo an toàn thông tin

1. Tổ chức mô hình mạng

- Cài đặt, cấu hình, quản trị hệ thống mạng nội bộ theo mô hình Clients/Server để kiểm soát máy trạm, hạn chế sử dụng mô hình mạng ngang hàng. Các cơ quan, đơn vị có nhiều phòng, ban, đơn vị trực thuộc không nằm

trong cùng một khu vực, cần thiết lập mạng riêng ảo để đảm bảo an ninh cho mạng nội bộ.

- Tùy vào điều kiện yêu cầu thực tế về bảo mật dữ liệu, các cơ quan chủ động triển khai xây dựng mô hình giải pháp an toàn bảo mật hệ thống mạng tại cơ quan cho phù hợp.

2. Quản lý phòng máy chủ (nếu có)

- Các thiết bị mạng quan trọng như tường lửa, thiết bị định tuyến, hệ thống máy chủ,...phải được đặt trong phòng máy chủ và có các biện pháp bảo vệ, ngăn chặn xâm nhập trái phép vào phòng máy chủ.

- Phòng máy chủ của các cơ quan là khu vực hạn chế tiếp cận, chỉ những người có trách nhiệm theo quy định của thủ trưởng cơ quan mới được phép vào phòng máy chủ.

- Phòng máy chủ nên được lắp đặt hệ thống điều hòa không khí, hệ thống camera giám sát. Quá trình vào, ra phòng máy chủ phải được ghi nhận vào nhật ký quản lý phòng máy chủ.

- Phòng máy chủ phải được trang bị đầy đủ thiết bị phòng chống cháy, nổ, hệ thống chống sét, có hệ thống ổn áp, lưu điện đủ công suất và duy trì thời gian hoạt động của các máy chủ tối thiểu 10 phút khi có sự cố mất điện.

3. Phòng chống mã độc

- Tất cả các máy trạm, máy chủ phải được trang bị phần mềm phòng chống mã độc. Các phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc khi sao chép, mở các tập tin.

- Các cán bộ, công chức, viên chức trong cơ quan phải được hướng dẫn về phòng chống mã độc, các rủi ro do mã độc gây ra.

- Tất cả các tập tin, thư mục phải được quét mã độc trước khi sao chép, sử dụng.

- Khi phát hiện ra bất kỳ dấu hiện nào liên quan đến việc bị nhiễm mã độc trên máy trạm (ví dụ: Máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu,...), người sử dụng phải tắt máy và báo trực tiếp cho bộ phận có trách nhiệm của đơn vị để xử lý.

4. Sao lưu dữ liệu dự phòng

- Các dữ liệu quan trọng của cơ quan phải được sao lưu, như: Thông tin cấu hình của hệ thống mạng, máy chủ; phần mềm ứng dụng và cơ sở dữ liệu; tập tin ghi nhật ký,...

- Các cơ quan phải lập kế hoạch và thực hiện sao lưu dữ liện phù hợp với điều kiện của từng cơ quan, đảm bảo khả năng phục hồi dữ liệu khi có sự cố xảy ra.

5. Quản lý thiết bị tường lửa

- Các hệ thống mạng phải được trang bị tường lửa, hệ thống phát hiện

và ngăn chặn xâm nhập để phát hiện và ngăn chặn các xâm nhập trái phép vào mạng nội bộ.

- Nhật ký hoạt động của thiết bị bảo mật phải được lưu giữ an toàn để phục vụ công tác khảo sát, điều tra khi có sự cố xảy ra.

6. Quản lý nhật ký trong quá trình vận hành các hệ thống thông tin

- Các cơ quan phải thực hiện việc ghi nhật ký (log) trên các thiết bị mạng máy tính, phần mềm ứng dụng, hệ điều hành, cơ sở dữ liệu nhằm đảm bảo các sự kiện quan trọng xảy ra trên hệ thống được ghi nhận và lưu giữ.

- Các nhật ký này phải được bảo vệ an toàn nhằm phục vụ công tác kiểm tra, phân tích khi cần thiết.

- Các sự kiện tối thiểu cần phải được ghi nhật ký gồm: quá trình đăng nhập hệ thống; tạo, cập nhật hoặc xóa dữ liệu; các hành vi xem, thiết lập cấu hình hệ thống; việc thiết lập các kết nối bất thường vào và ra hệ thống; thay đổi quyền truy cập hệ thống.

- Thường xuyên thực hiện việc theo dõi bản ghi nhật ký của 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.

7. Quản lý truy cập

- Các quy định về quản lý truy cập vào hệ thống thông tin, mạng máy tính, thiết bị, phần mềm ứng dụng của đơn vị phải được quy định chi tiết và tổ chức thực hiện nghiêm túc, phù hợp với các quy định của pháp luật về an toàn thông tin.

- Mỗi tài khoản truy cập các hệ thống thông tin chỉ được cấp cho một người quản lý và sử dụng.

- Mỗi cán bộ, công chức, viên chức chỉ được phép truy cập các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình, có trách nhiệm bảo mật tài khoản truy cập thông tin.

- Các hệ thống thông tin cần giới hạn số lần đăng nhập sai liên tiếp vào hệ thống. Hệ thống tự động khoá 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.

- Tất cả máy trạm, máy chủ phải được đặt mật khẩu truy cập và thiết lập khóa tài khoản khi không sử dụng.

- Khi thiết lập mạng không dây trong nội bộ đơn vị, phải đặt mật khẩu truy cập vào mạng không dây và chỉ cho phép truy cập Internet.

- Các tài khoản người dùng liên quan đến hệ thống CNTT của cơ quan phải được đặt mật khẩu truy cập. Mật khẩu truy cập vào các hệ thống thông tin phải có độ phức tạp cao và phải được thay đổi thường xuyên.

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 9. Trách nhiệm của Sở Thông tin và Truyền thông

1. Tham mưu UBND tỉnh về công tác đảm bảo an toàn thông tin trên địa bàn tỉnh và chịu trách nhiệm trước UBND tỉnh trong việc đảm bảo an toàn an ninh cho các hệ thống thông tin của tỉnh.

2. Hằng năm xây dựng kế hoạch triển khai công tác đảm bảo an toàn thông tin phục vụ cho việc vận hành các hệ thống thông tin được UBND tỉnh giao quản lý.

3. Chủ trì, phối hợp với Công an tỉnh và các cơ quan, đơn vị liên quan tổ chức kiểm tra theo định kỳ hoặc đột xuất; kịp thời phát hiện và xử lý theo quy định của pháp luật đối với các cơ quan, tổ chức, cá nhân có các dấu hiệu, hành vi vi phạm an toàn thông tin trên địa bàn tỉnh.

4. Hằng năm xây dựng và triển khai các chương trình đào tạo chuyên sâu về an toàn thông tin cho lực lượng đảm bảo an toàn thông tin của các cơ quan, đơn vị.

5. Tổ chức các hội nghị, hội thảo chuyên đề và tuyên truyền về an toàn thông tin trong công tác quản lý Nhà nước trên địa bàn tỉnh.

6. Tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin của tỉnh.

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

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

9. Tổng hợp và báo cáo về tình hình an toàn thông tin theo định kỳ cho Bộ Thông tin và Truyền thông, UBND tỉnh và các cơ quan, đơn vị có liên quan.

10. Xây dựng bảng tiêu chí đánh giá xếp hạng an toàn thông tin.

Điều 10. Trách nhiệm của Công an tỉnh

1. Chủ trì, phối hợp với Sở Thông tin và Truyền thông và các cơ quan, đơn vị có liên quan xây dựng kế hoạch và chịu trách nhiệm kiểm soát, phòng ngừa, đấu tranh, ngăn chặn các loại tội phạm lợi dụng hệ thống thông tin gây hại đến an toàn, an ninh thông tin trong cơ quan nhà nước.

2. Phối hợp với các cơ quan chức năng trong trao đổi biện pháp kỹ thuật, kiểm tra, đánh giá nhằm đảm bảo an toàn, an ninh thông tin.

3. Tăng cường công tác phòng ngừa, phát hiện và tuyên truyền, phổ biến pháp luật về xử lý tội phạm trong việc đảm bảo an toàn, an ninh

thông tin.

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

5. Thực hiện nhiệm vụ bảo vệ an toàn các công trình quan trọng về an ninh quốc gia trên địa bàn tỉnh.

Điều 11. Trách nhiệm của 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 trước UBND tỉnh trong công tác đảm bảo an toàn thông tin của đơn vị mình.

2. Phân công cán bộ có chuyên môn phụ trách an toàn thông tin của cơ quan; tạo điều kiện để các cán bộ phụ trách an toàn thông tin được học tập, nâng cao trình độ về an toàn thông tin, hệ thống mạng; tạo điều kiện cho cán bộ, công chức, viên chức được tham gia các lớp tập huấn về kiến thức an toàn thông tin.

3. Xây dựng quy định, quy trình nội bộ về bảo đảm an toàn thông tin phù hợp với Quy chế này và các quy định của pháp luật, đồng thời đáp ứng các tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin.

4. Khi thực hiện đầu tư, triển khai các dự án ứng dụng công nghệ thông tin cần có giải pháp cụ thể để đảm bảo an toàn thông tin cho hệ thống thông tin đáp ứng các yêu cầu về tiêu chuẩn kỹ thuật, an toàn bảo mật.

5. Phối hợp, cung cấp thông tin và tạo điều kiện cho các đơn vị có thẩm quyền triển khai công tác kiểm tra khắc phục sự cố xảy ra một cách kịp thời, nhanh chóng và đạt hiệu quả.

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

7. Báo cáo định kỳ trước ngày 15 tháng 12 hàng năm hoặc đột xuất về tình hình an toàn thông tin của cơ quan và gửi về Sở Thông tin và Truyền thông.

Điều 12. Trách nhiệm của cán bộ, công chức, viên chức trong các cơ quan

1. Trách nhiệm của cán bộ, công chức, viên chức phụ trách an toàn thông tin

- Chịu trách nhiệm đảm bảo an toàn thông tin của đơn vị;

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

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

- 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 thông tin.

2. Trách nhiệm của cán bộ, công chức, viên chức trong các cơ quan, đơn vị

- Nghiêm túc chấp hành các quy định, quy trình nội bộ, Quy chế này và các quy định khác của pháp luật về an toàn thông tin. Chịu trách nhiệm đảm bảo an toàn thông tin trong phạm vi trách nhiệm và quyền hạn được giao;

- Mỗi cán bộ, công chức, viên chức phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp các thiết bị trên máy tính; không được vào các trang web không rõ về nội dung; không tải và cài đặt các phần mềm không rõ nguồn gốc, không liên quan đến công việc chuyên môn; không nhấp chuột vào các đường dẫn lạ không rõ về nội dung;

- Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin phải báo cáo ngay với cấp trên và bộ phận chuyên trách CNTT của đơn vị để kịp thời ngăn chặn và xử lý;

- Tham gia các chương trình đào tạo, hội nghị về an toàn an ninh thông tin.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 13. Khen thưởng và xử lý vi phạm

1. Hằng 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 để đánh giá, xếp hạng an toàn thông tin, trên cơ sở đó đề xuất UBND tỉnh xem xét khen thưởng theo quy định hiện hành.

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

Điều 14. Điều khoản thi hành

1. Thủ trưởng các sở, ban, ngành tỉnh, Chủ tịch UBND các huyện, thành phố chịu trách nhiệm tổ chức triển khai thực hiện Quy chế tại đơn vị mình.

2. Trong quá trình thực hiện, nếu có những vấn đề cần sửa đổi, bổ sung, đề nghị các đơn vị gửi về Sở Thông tin và Truyền thông để tổng hợp, báo cáo UBND tỉnh xem xét, quyết định./.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Nguyễn Hoàng Anh