ỦY BAN NHÂN DÂN TỈNH QUẢNG BÌNH	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 26/2014/QĐ-UBND	*Quảng Bình, ngày 21 tháng 10 năm 2014*

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

ỦY BAN NHÂN DÂN TỈNH QUẢNG BÌNH

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

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 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;

Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Tờ trình số 650/TTr-STTTT ngày 16 tháng 9 năm 2014,

QUYẾT ĐỊNH:

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

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

Điều 3. Chánh Văn phòng UBND tỉnh; Giám đốc Sở Thông tin và Truyền thông; Thủ trưởng các sở, ban, ngành cấp tỉnh; Chủ tịch UBND huyện, thị xã, thành phố; Chủ tịch UBND 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./.

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;
- Đoàn Đại biểu Quốc hội tỉnh;
- UBMTTQVN tỉnh;
- CT, các PCT UBND tỉnh;
- Sở Tư pháp;
- Báo Quảng Bình, Đài PTTH Quảng Bình;
- Trung tâm tin học - Công báo tỉnh;
- Lưu: VT, VX.

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

(Đã ký)

Nguyễn Tiến Hoàng

ỦY BAN NHÂN DÂN TỈNH QUẢNG BÌNH	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc

QUY CHẾ
Đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Quảng Bình

(Ban hành kèm theo Quyết định số: 26/2014/QĐ-UBND ngày 21 tháng 10 năm 2014 của Ủy ban nhân dân tỉnh Quảng Bình)

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 trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Quảng Bình.

Điều 2. Đối tượng áp dụng

1. Các sở, ban, ngành; Ủy ban nhân huyện, thị xã, thành phố; các đơn vị sự nghiệp thuộc tỉnh; Ủy ban nhân dân 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 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. 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 số của tỉnh.

2. Trung tâm Dữ liệu điện tử của tỉnh: là một công trình xây dựng, bao gồm nhà trạm, hệ thống cáp và hệ thống máy tính cùng các thiết bị phụ trợ lắp đặt vào đó để lưu trữ, trao đổi và quản lý tập trung dữ liệu của tỉnh.

3. An toàn thông tin: là sự bảo vệ thông tin và các hệ thống thông tin 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.

Chương II

NỘI DUNG ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 4. Các quy định chung về đảm bảo an toàn thông tin

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. 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.

4. 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.

5. 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.

Điều 5. Đảm bảo an toàn thông tin cho các hệ thống thông tin và các thiết bị công nghệ thông tin

1. Sở Thông tin và Truyền thông có trách nhiệm đảm bảo an toàn thông tin cho các hệ thống thông tin, bao gồm:

a) Nghiên cứu và đề xuất xây dựng các hệ thống ứng dụng công nghệ thông tin dùng chung trên địa bàn tỉnh để tăng hiệu quả sử dụng, tiết kiệm đầu tư, đảm bảo tính liên thông giữa các cơ quan, đơn vị và thuận tiện trong việc đảm bảo an toàn thông tin;

b) Tổ chức thực hiện đánh giá an toàn thông tin cho các hệ thống thông tin dùng chung của tỉnh;

c) Chịu trách nhiệm giám sát và đảm bảo an toàn thông tin cho các hệ thống thông tin của tỉnh, đặc biệt là các hệ thống cơ sở dữ liệu quan trọng, Cổng/trang thông tin điện tử, thư điện tử, quản lý văn bản, một cửa điện tử, quản lý nhân sự, báo cáo trực tuyến;

d) Chủ trì, phối hợp với các cơ quan, đơn vị trong tỉnh để thực hiện quản lý chặt chẽ tài khoản người dùng của các hệ thống thông tin. Đối với cán bộ, công chức, viên chức đã nghỉ việc, chuyển công tác, phải có biện pháp khóa hoặc hủy

tài khoản, quyền truy nhập, thu hồi các thiết bị liên quan tới hệ thống thông tin (khóa, thẻ nhận dạng,...);

e) Chủ trì, phối hợp với các cơ quan, đơn vị liên quan tổ chức lên phương án sao lưu và phục hồi dữ liệu khi xảy ra sự cố đối với các hệ thống thông tin của tỉnh; tổ chức sao lưu dữ liệu các hệ thống dùng chung của tỉnh và hướng dẫn về sao lưu dự phòng các dữ liệu quan trọng.

f, Tham mưu Ủy ban nhân dân tỉnh hướng dẫn việc sử dụng các thiết bị viễn thông, máy tính dùng để lưu giữ và truyền thông tin bí mật nhà nước.

2. Các cơ quan, đơn vị nếu triển khai các hệ thống thông tin độc lập thì phải tự chịu trách nhiệm đảm bảo an toàn thông tin và phối hợp với Sở Thông tin và Truyền thông khi được yêu cầu.

3. Đảm bảo an toàn thông tin cho các hệ thống thiết bị mạng, máy chủ, máy tính cá nhân và các hệ thống lưu trữ:

a) Máy chủ, máy tính cá nhân, hệ thống lưu trữ nội bộ, thiết bị mạng phải được bảo vệ bởi mật khẩu an toàn, tuyệt đối không sử dụng mật khẩu ngắn, mặc định;

b) 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;

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 của virus tại cơ quan, đơn vị mình phải báo cáo tình hình về Sở Thông tin và Truyền thông thông qua đường dây nóng;

e) Khi xảy ra sự cố máy tính có tính chất nghiêm trọng 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 khắc phục ngay sự cố.

Điều 6. Đảm bảo an toàn thông tin cho Trung tâm Dữ liệu điện tử của tỉnh

1. Sở Thông tin và Truyền thông có trách nhiệm đảm bảo an toàn cho Trung tâm Dữ liệu điện tử của tỉnh.

2. Các cơ quan, đơn vị đặt dữ liệu hoặc kết nối vào Trung tâm Dữ liệu điện tử phải tuân thủ các chính sách an toàn thông tin liên quan đến việc kết nối vào Trung tâm Dữ liệu điện tử do Sở Thông tin và Truyền thông hướng dẫn.

3. Các cơ quan, đơn vị khi kết nối vào Trung tâm Dữ liệu phải tự bảo vệ hệ thống đầu cuối của mình và phải chịu trách nhiệm nếu để tin tặc kiểm soát máy tính và tấn công ngược vào Trung tâm Dữ liệu điện tử.

4. Sở Thông tin và Truyền thông xây dựng phương án đảm bảo an toàn thông tin cho dữ liệu của các cơ quan, đơn vị đặt tại Trung tâm Dữ liệu điện tử nhưng phải đảm bảo thuận lợi cho việc truy xuất và sử dụng các dữ liệu này.

5. Sở Thông tin và Truyền thông đảm bảo các điều kiện về hạ tầng kỹ thuật, an toàn thông tin đối với hệ thống máy chủ, thiết bị kết nối mạng đặt tại Trung tâm Dữ liệu điện tử.

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 7. Trách nhiệm của các cơ quan, đơn vị

1. 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.

2. Thủ trưởng các cơ quan, đơn vị có trách nhiệm tuyên truyền, nâng cao nhận thức cho cán bộ, công chức, viên chức về các nguy cơ mất an toàn hệ thống thông tin; 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 của cơ quan, đơn vị mình.

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

4. Quan tâm và ưu tiên 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 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; 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 8. Trách nhiệm của Sở Thông tin và Truyền thông

1. Tham mưu 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 cấp 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 cho các cơ quan, đơn vị trong tỉnh.

4. 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 của tỉnh và hỗ trợ các cơ quan, đơn vị trong tỉnh xử lý sự cố mất an toàn thông tin.

5. 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.

6. 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.

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

8. 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 khi có yêu cầu.

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.

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

Điều 9. 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.

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

Tham mưu UBND tỉnh bố trí kinh phí để đầu tư, quản lý, duy trì, vận hành các hệ thống an toàn thông tin của tỉnh.

Điều 11. 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 7 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 gắn với việc đảm bảo an toàn thông tin.

b) Viễn thông Quảng Bình 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 12. 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 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.

b) 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.

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) Khi phát hiện sự cố 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 do Sở Thông tin và Truyền thông hoặc các cơ quan, đơn vị chuyên môn tổ chức.

Chương IV

CÔNG TÁC THANH TRA, KIỂM TRA AN TOÀN THÔNG TIN

Điều 13. Kế hoạch thanh tra, kiểm tra hàng năm

1. Định kỳ hàng năm tối thiểu 1 lần vào quý III hoặc quý IV, tiến hành kiểm tra đột xuất các cơ quan, đơn vị khi có dấu hiệu vi phạm an toàn thông tin.

2. Sở Thông tin và Truyền thông chủ trì, phối hợp Công an tỉnh và các cơ quan, đơn vị có liên quan để tham mưu thành lập Đoàn kiểm tra; xây dựng kế hoạch kiểm tra và tiến hành công tác kiểm tra an toàn thông tin tại tất cả các cơ quan, đơn vị.

Chủ trì hoạt động thanh tra và xử lý các hành vi vi phạm về an toàn thông tin và phát tán tin nhắn rác trên địa bàn tỉnh. Phối hợp với Công an tỉnh tiến hành xử phạt các hành vi vi phạm an toàn thông tin gây thiệt hại cho hệ thống thông tin thuộc các cơ quan, đơn vị nhà nước thuộc tỉnh.

Chương V

TỔ CHỨC THỰC HIỆN

Điều 14. 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 để lập bảng xếp hạng an toàn thông tin, trên cơ sở đó đề xuất UBND tỉnh xem xét khen thưởng theo quy định.

2. Các cơ quan, đơn vị, cá nhân 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.

Điều 15. Điều khoản thi hành

Sở Thông tin và Truyền thông có trách nhiệm hướng dẫn triển khai thực hiện Quy chế này.

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./.