ỦY BAN NHÂN DÂN TỈNH HÀ GIANG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 1374 /QĐ-UBND	*Hà Giang, ngày 24 tháng 7 năm 2017*

QUYẾT ĐỊNH
Ban hành Quy chế đảm bảo an toàn thông tin mạng trên địa bàn tỉnh Hà Giang

CHỦ TỊCH ỦY BAN NHÂN DÂN TỈNH HÀ GIANG

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 An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

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 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.

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 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.

Xét đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Tờ trình số 24/TTr-STTTT ngày 29 tháng 6 năm 2017,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế đảm bảo an toàn thông tin mạng trên địa bàn tỉnh Hà Giang.

Điều 2. Quyết định này có hiệu lực kể từ ngày ký.

Điều 3. Chánh Văn phòng UBND tỉnh, Thủ trưởng các sở, ban, ngành, đoàn thể của tỉnh; Chủ tịch UBND các huyện, thành phố và các tổ chức, cá nhân liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Bộ Thông tin và Truyền thông;
- Thường trực Tỉnh ủy,
- Thường trực HĐND;
- Chủ tịch, các PCT UBND tỉnh;
- Văn phòng Tỉnh ủy, HĐND, UBND tỉnh;
- Cổng thông tin điện tử tỉnh;
- Trung tâm Công báo - Tin học tỉnh;
- Lưu: VT, KTN.

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Trần Đức Quý

ỦY BAN NHÂN DÂN TỈNH HÀ GIANG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc

QUY CHẾ
Đảm bảo an toàn thông tin mạng trên địa bàn tỉnh Hà Giang

(Ban hành kèm theo Quyết định số: 1374/QĐ-UBND ngày 24 tháng 7 năm 2017 của UBND tỉnh Hà Giang)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về đảm bảo an toàn thông tin mạng trên địa bàn tỉnh Hà Giang.

Điều 2. Đối tượng áp dụng

1. Các cơ quan Đảng, Mặt trận Tổ quốc và các đoàn thể; các Sở, Ban, Ngành, Công an tỉnh, UBND các huyện, thành phố; các đơn vị sự nghiệp công lập; UBND các xã, phường, thị trấn; các doanh nghiệp viễn thông và công nghệ thông tin (sau đây gọi tắt là cơ quan, đơn vị);

2. Cán bộ, công chức, viên chức và người lao động đang công tác trong các cơ quan, đơn vị nêu tại Khoản 1 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 dùng chung của tỉnh, hệ thống thông tin tại các cơ quan, đơn vị.

Chương II
NỘI DUNG BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 3. Đảm bảo an toàn hạ tầng ứng dụng công nghệ thông tin

1. Đảm bảo an toàn thông tin chung cho hệ thống thông tin, hệ thống thiết bị mạng, máy chủ, máy tính cá nhân:

a) Lãnh đạo cơ quan, đơn vị chịu trách nhiệm chỉ đạo thực hiện giải pháp bảo vệ an toàn vật lý cho các 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)... 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 định kỳ thay đổi ít nhất 03 (ba) tháng/lần.

c) Quản lý đăng nhập hệ thống: Các hệ thống thông tin cần giới hạn số lần đăng nhập vào hệ thống, tự động khóa tài khoản khi liên tục đăng nhập sai vượt quá số lần nhất định. Tổ chức theo dõi, các phương pháp đăng nhập từ xa, đặc biệt các trường hợp đăng nhập vào hệ thống với mục đích quản trị.

d) Chống phần mềm độc hại: Triển khai các phần mềm chống mã độc trên các máy tính, thiết bị di động trong mạng để phát hiện, loại trừ phần mềm 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 thường xuyên ít nhất 01 (một) lần/tuần. Thường xuyên cập nhật bản vá các lỗ hổng bảo mật của hệ điều hành và các phần mềm ứng dụng trên máy tính để hạn chế tối đa rủi ro mất an toàn thông tin.

đ) Khi xảy ra sự cố an toàn thông tin mạng, cơ quan, đơn vị có trách nhiệm thông báo kịp thời cho doanh nghiệp cung cấp dịch vụ hoặc bộ phận chuyên trách ứng cứu sự cố để 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.

e) Quản lý nhật ký sự kiện (logfile): Hệ thống thông tin cần ghi nhận các sự kiện: quá trình đăng nhập hệ thống, các thao tác cấu hình hệ thống, quá trình truy xuất hệ thống... Thường xuyên kiểm tra, sao lưu (backup) các nhật ký sự kiện theo từng tháng để theo dõi, xác định những sự kiện đã xảy ra của hệ thống và hạn chế việc tràn nhật ký sự kiện gây ảnh hưởng đến hoạt động của hệ thống.

g) Xử lý khẩn cấp: Khi phát hiện hệ thống thông tin trên mạng bị tấn công cần thực hiện các bước cơ bản sau:

Bước 1: Ngắt kết nối máy chủ ra khỏi mạng.

Bước 2: Xác minh tình trạng, mức độ, phạm vi sự cố, sau đó phân loại sự cố (tấn công thay đổi giao diện, tấn công lừa đảo, tấn công phát tán mã độc, tấn công từ chối dịch vụ...)

Bước 3: Sao chép nhật ký sự kiện và toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ (phục vụ cho hoạt động phân tích, điều tra). Đối với trường hợp phức tạp không tự xử lý được, thực hiện ngay Bước 4.

Bước 4: Báo cáo kịp thời cho lãnh đạo cơ quan, đơn vị và Sở Thông tin và Truyền thông để kịp thời phối hợp xử lý sự cố.

Bước 5: Khôi phục hệ thống bằng cách chuyển dữ liệu sao lưu mới nhất để hệ thống hoạt động trở lại. Lưu trữ hồ sơ xử lý sự cố.

2. Đảm bảo an toàn với các đơn vị có hệ thống thông tin riêng:

a) Các cơ quan, đơn vị có hệ thống thông tin riêng của ngành, đơn vị, địa phương thực hiện 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) 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...

d) 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 theo điểm c), d), đ), e) Khoản 1 Điều này.

đ) 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,... được 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 4. 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, đặc biệt 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 Công nghệ thông tin liên quan.

Điều 5. Đảm bảo an toàn thông tin cho Trung tâm tích hợp Dữ liệu của tỉnh

Thực hiện theo Quyết định số 2276/QĐ-UBND ngày 23/9/2016 của UBND tỉnh Hà Giang ban hành Quy chế quản lý, vận hành và khai thác Trung tâm tích hợp dữ liệu tỉnh Hà Giang.

Điều 6. Phát triển nguồn nhân lực an toàn thông tin

1. Công chức, viên chức 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. Công chức, viên chức 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 khóa đào tạo nhân lực trong lĩnh vực an toàn thông tin mạng.

Chương III
TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 7. Trách nhiệm của Sở Thông tin và Truyền thông

1. UBND tỉnh ủy quyền cho Sở Thông tin và Truyền thông quản lý an toàn thông tin trong hoạt động ứng dụng dụng CNTT dùng chung trên hạ tầng Trung tâm tích hợp dữ liệu của tỉnh; và các ứng dụng CNTT khác trên địa bàn tỉnh.

2. Tham mưu giúp Ủy ban nhân dân tỉnh thành lập Ban chỉ đạo ứng cứu khẩn cấp an toàn thông tin mạng. Trong đó: Trưởng ban là Giám đốc Sở Thông tin và Truyền thông; Phó trưởng ban là Giám đốc Trung tâm CNTT&TT và các thành viên khác là công chức, viên chức chuyên trách về CNTT tại các cơ quan nhà nước trên địa bàn tỉnh. Cơ quan thường trực Ban chỉ đạo là Trung tâm CNTT&TT tỉnh Hà Giang.

3. Hàng năm xây dựng kế hoạch, dự toán nguồn kinh phí để triển khai công tác bảo đảm an toàn thông tin cho các hệ thống thông tin được Ủy ban nhân dân tỉnh giao quản lý.

4. Chủ trì, phối hợp với các cơ quan liên quan thành lập đoàn kiểm tra an toàn thông tin định kỳ hàng năm hoặc kiểm tra đột xuất khi phát hiện có các dấu hiệu vi phạm an toàn thông tin.

5. Chịu trách nhiệm xây dựng và trình Ủy ban nhân dân tỉnh ban hành các quy định và hướng dẫn, khuyến nghị về đảm bảo an toàn thông tin mạng cho các cơ quan, đơn vị.

6. 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.

7. Hướng dẫn, giám sát các đơn vị xây dựng quy chế, quy trình bảo đảm an toàn cho hệ thống thông tin theo quy định của Nhà nước; 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 mạng.

8. Nghiên cứu, tham mưu UBND 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.

9. Xây dựng và triển khai các chương trình đào tạo, tổ chức các hội nghị, hội thảo về an toàn thông tin mạng nhằm phổ biến, cập nhật kiến thức về an toàn thông tin.

10. 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 8. 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 với Sở Thông tin và Truyền thông thanh tra, kiểm tra công tác bảo đảm an toàn thông tin đối với các cơ quan, đơn vị trên địa bàn tỉnh.

3. Kịp thời thông báo, trao đổi với 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.

4. Thực hiện nhiệm vụ bảo vệ an toàn các công trình quan trọng về an ninh quốc gia; hạ tầng cơ sở lĩnh vực công nghệ thông tin trên địa bàn tỉnh.

Điều 9. 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. Trang bị 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.

3. 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.

4. Khi có sự cố an toàn thông tin mạng hoặc có nguy cơ mất an toàn thông tin kịp thời chỉ đạo công chức, viên chức chuyên trách CNTT khắc phục ngay, kịp thời thông báo cho doanh nghiệp cung cấp dịch vụ và Sở Thông tin và Truyền thông bằng văn bản, để phối hợp thực hiện.

5. 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.

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 chịu trách nhiệm đảm bảo an toàn thông tin cho hệ thống công nghệ thông tin của cơ quan, đơn vị mình.

8. Báo cáo Ủy ban nhân dân tỉnh (*thông qua Sở Thông tin và Truyền thông*) 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).

Điều 10. Trách nhiệm của Sở Tài chính

Phối hợp với Sở Thông tin và Truyền thông tham mưu cho Ủy ban nhân dân tỉnh trong việc bố trí kinh phí cho các hoạt động đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh.

Điều 11. Trách nhiệm của cán bộ, công chức, viên chức, người lao động trong các cơ quan, đơn vị

1. Trách nhiệm của bộ phận 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 Ủy ban nhân dân tỉnh tổ chức.

2. Đối với cán bộ, công chức, viên chức, người lao động:

a) Thường xuyên cập nhật, nghiêm túc chấp hành những chính sách, quy trình, thủ tục an toàn thông tin mạng của đơn vị và hướng dẫn về an toàn thông tin của cán bộ chuyên trách công nghệ thông tin, nâng cao ý thức cảnh giác và trách nhiệm đảm bảo an toàn thông tin tại cơ quan, đơn vị.

b) Hạn chế việc sử dụng chức năng chia sẻ tài nguyên, khi 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. 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.

c) Các tài khoản đăng nhập hệ điều hành thực hiện đặt mật khẩu an toàn, khi không sử dụng thì khóa tài khoản. Trường hợp không sử dụng máy tính trong thời gian quá 02 (hai) giờ cần tắt máy hoặc ngắt kết nối mạng để tránh bị các tin tặc lợi dụng, điều khiển máy tính từ xa.

d) Sử dụng chức năng mã hóa ở mức hệ điều hành để bảo đảm các dữ liệu nhạy cảm như tài khoản, mật khẩu, các tập tin quan trọng,... được mã hóa. Các tập tin hoặc sao chép từ thiết bị lưu trữ cần được kiểm tra để tránh đính kèm thư điện tử, tải xuống từ Internet lây nhiễm các phần mềm độc hại.

đ) Không sử dụng tên tài khoản công vụ làm tên tài khoản các mạng xã hội, các diễn đàn và các trang thông tin khác trên mạng Internet. Chỉ sử dụng thư điện tử công vụ trong các hoạt động công vụ.

e) Không cài đặt phần mềm không rõ nguồn gốc. Tuân thủ các quy định về bảo đảm an toàn sử dụng thư điện tử.

f) 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.

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

Điều 12. Điều khoản thi hành

Sở Thông tin và Truyền thông chủ trì, phối hợp với các Sở, Ban, Ngành, UBND các huyện, thành phố và các cơ quan có liên quan triển khai thực hiện Quy chế này.

Trong quá trình thực hiện nếu có phát sinh khó khăn, vướng mắc cần sửa đổi, bổ sung các cơ quan, đơn vị kịp thời phản ánh về Sở Thông tin và Truyền thông tổng hợp, báo cáo Ủy ban nhân dân tỉnh xem xét sửa đổi, bổ sung Quy chế cho phù hợp./.

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Trần Đức Quý