ỦY BAN NHÂN DÂN TỈNH BÀ RỊA – VŨNG TÀU	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 327 /QĐ-UBND	*Bà Rịa -Vũng Tàu, ngày 31 tháng 01 năm 2013*

QUYẾT ĐỊNH

Ban hành Hướng dẫn đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan Nhà nước tỉnh Bà Rịa-Vũng Tàu.

CHỦ TỊCH ỦY BAN NHÂN DÂN TỈNH BÀ RỊA VŨNG TÀU

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 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 Quyết định số 63/QĐ-TTg ngày 13 tháng 01 năm 2010 của Thủ tướng Chính phủ về việc phê duyệt Quy hoạch phát triển an toàn thông tin số quốc gia đến năm 2020;

Căn cứ Chỉ thị số 879/CT-TTg ngày 10 tháng 6 năm 2011 của Thủ tướng chính phủ về việc tăng cường triển khai các hoạt động đảm bảo an toàn thông tin số;

Căn cứ Quyết định số 238/QĐ-UBND ngày 25 tháng 01 năm 2011 của UBND Tỉnh phê duyệt kế hoạch Ứng dụng công nghệ thông tin trong hoạt động của cơ quan Nhà nước trên địa bàn tỉnh Bà Rịa-Vũng Tàu giai đoạn 2011-2015;

Căn cứ Quyết định số 1396/QĐ-UBND ngày 23 tháng 6 năm 2011 của UBND Tỉnh phê duyệt phê duyệt kế hoạch triển khai đề án Đưa Việt Nam sớm trở thành nước mạnh về Công nghệ thông tin – Truyền thông tại tỉnh Bà Rịa-Vũng Tàu,

Xét đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Tờ trình số 03/TTr-STTTT ngày 04 tháng 01 năm 2013 về việc ban hành Quyết định Hướng dẫn đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước thuộc UBND tỉnh Bà Rịa-Vũng Tàu.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Hướng dẫn đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước thuộc tỉnh Bà Rịa-Vũng Tàu.

Bản Hướng dẫn gồm có 4 chương, 12 điều.

Điều 2. Chánh Văn phòng Ủy ban nhân dân Tỉnh, Giám đốc Sở Thông tin và Truyền thông, Giám đốc Công an Tỉnh, Giám đốc các sở, ban, ngành, Chủ tịch UBND các huyện, thành phố và Thủ trưởng các đơn vị có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Bộ TT&TT (b/c);
- TTrTU, TTr HĐND tỉnh (b/c);
- CT, các PCT UBND tỉnh;
- Như điều 2 ;
- Lưu VT, CNTT

CNTT 24/01/13

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Lê Thanh Dũng

ỦY BAN NHÂN DÂN TỈNH BÀ RỊA -VŨNG TÀU	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc

HƯỚNG DẪN

Đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan Nhà nước thuộc tỉnh Bà Rịa-Vũng Tàu.

(Ban hành kèm theo Quyết định số: 327/QĐ-UBND ngày 31 tháng 01 năm 2013 của Chủ tịch UBND tỉnh Bà Rịa- Vũng Tàu)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Mục đích, yêu cầu

- Mục đích: Hướng dẫn này nhằm đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan Nhà nước trên địa bàn tỉnh Bà Rịa - Vũng Tàu bao gồm các sở, ban, ngành, Ủy ban nhân dân các huyện, thành phố thuộc tỉnh Bà Rịa - Vũng Tàu *(gọi tắt là các cơ quan thuộc Tỉnh)*

- Yêu cầu: Các cơ quan thuộc Tỉnh áp dụng Hướng dẫn này trong việc vận hành, khai thác và sử dụng hệ thống công nghệ thông tin tại các cơ quan, đơn vị.

Điều 2. Giải thích từ ngữ

1. An toàn thông tin số: là thuật ngữ dùng để chỉ việc bảo vệ thông tin số và các hệ thống thông tin phòng tránh các nguy cơ do tự nhiên, các hành động truy cập, sử dụng, phát tán, phá hoại, sửa đổi và phá hủy bất hợp pháp nhằm đảm bảo cho các hệ thống thông tin thực hiện đúng chức năng, phục vụ đúng đối tượng một cách sẵn sàng, chính xác và tin cậy. Nội dung của an toàn thông tin bao gồm bảo vệ an toàn mạng và hạ tầng thông tin, an toàn máy tính, dữ liệu và ứng dụng công nghệ thông tin.

2. Hệ thống thông tin: là một tập hợp và kết hợp các phần cứng, phần mềm, các hệ thống mạng truyền thông được xây dựng và sử dụng để thu nhập, tạo và tái tạo, phân phối và chia sẻ các dữ liệu, thông tin, tri thức nhằm phục vụ cho các mục tiêu của tổ chức.

3. An toàn, an ninh thông tin: là đảm bảo thông tin được bảo mật, sẵn sàng và toàn vẹn.

4. Tính tin cậy: là đảm bảo thông tin chỉ có thể được truy cập bởi những người được cấp quyền truy cập.

5. Tính toàn vẹn: là bảo vệ tính chính xác, tính đầy đủ của thông tin và các phương pháp xử lý thông tin.

6. Tính sẵn sàng: là đảm bảo những người được cấp quyền có thể truy cập thông tin và các tài liệu có liên quan ngay khi có nhu cầu.

7. Môi trường mạng bao gồm: mạng nội bộ (LAN); mạng diện rộng (WAN), mạng Truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước, mạng riêng ảo (VPN), mạng Internet và các dịch vụ mạng khác.

8. TCVN 7562:2005 Tiêu chuẩn Việt Nam về mã thực hành quản lý an toàn thông tin.

9. TCVN ISO/IEC 27001:2009 : Tiêu chuẩn Việt Nam về quản lý an toàn thông tin số.

10. Các cơ quan, đơn vị: là cụm từ viết tắt chỉ các sở, ban, ngành, Ủy ban nhân dân các huyện, thành phố.

Chương II
ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 3. Những quy định đảm bảo an toàn, an ninh thông tin

1. Các cơ quan, đơn vị phải phổ biến những kiến thức cơ bản về an toàn, an ninh thông tin cho cán bộ, công chức, viên chức và người lao động trước khi tham gia sử dụng hệ thống thông tin.

2. Bố trí người làm công tác chuyên trách về công nghệ thông tin phải có chuyên ngành phù hợp và được đào tạo, bồi dưỡng chuyên môn đối với lĩnh vực an toàn, an ninh thông tin.

3. Hàng năm bố trí kinh phí với mức từ 10% đến 20 % trở lên của tổng kinh phí đầu tư ứng dụng công nghệ thông tin của cơ quan, đơn vị cho hạng mục về an toàn, an ninh thông tin.

4. Cán bộ tham gia đoàn kiểm tra công tác đảm bảo an toàn, an ninh thông tin phải được trang bị đầy đủ những kiến thức và được tập huấn hàng năm về công tác an toàn, an ninh thông tin.

5. Các cơ quan, đơn vị phải xây dựng, ban hành quy chế nội bộ đảm bảo an ninh, an toàn thông tin, và căn cứ theo các nội dung của tiêu chuẩn TCVN 7562:2005 và TCVN ISO/IEC 27001:2009. Quy chế khi xây dựng có nội dung quy định các vấn đề sau:

a) Mục tiêu.

b) Quy định cụ thể quyền và trách nhiệm của từng đối tượng: lãnh đạo đơn vị, lãnh đạo phòng, cán bộ chuyên trách về công nghệ thông tin, người sử dụng.

c) Quy định về cấp phát, thu hồi, cập nhật và quản lý các tài khoản truy cập vào hệ thống thông tin.

d) Quy định về an toàn, an ninh thông tin trên môi trường mạng nội bộ.

đ) Cơ chế sao lưu dữ liệu, cơ chế thông tin, báo cáo và phối hợp khắc phục sự cố.

e) Theo dõi, kiểm tra, thống kê, tổng hợp, báo cáo theo định kỳ và đột xuất.

g) Khen thưởng, kỷ luật.

h) Tổ chức thực hiện.

6. Các cơ quan, đơn vị xây dựng, triển khai kế hoạch đảm bảo an toàn, an ninh thông tin và tổng hợp báo cáo về Sở Thông tin và Truyền thông theo định kỳ hàng năm.

Điều 4. Quản lý, vận hành hệ thống thông tin của cơ quan, đơn vị

1. Hệ thống thông tin của các cơ quan, đơn vị phải có cơ chế sao lưu (backup) tất cả dữ liệu của các ứng dụng và dữ liệu người sử dụng. Cơ chế sao lưu dữ liệu phải được thực hiện thường xuyên. Thiết bị lưu trữ dữ liệu phải đảm bảo yêu cầu kỹ thuật. Dữ liệu được sao lưu phải đảm bảo tính sẵn sàng và toàn vẹn đáp ứng yêu cầu phục hồi dữ liệu cho hệ thống thông tin hoạt động bình thường khi có sự cố xảy ra.

2. Hệ thống thông tin của các cơ quan, đơn vị phải được triển khai cơ chế bảo mật và an toàn thông tin bằng các thiết bị phần cứng và phần mềm, bao gồm:

a) Đầu tư trang bị các thiết bị phần cứng về bảo mật (firewall) phù hợp với quy mô hệ thống thông tin của cơ quan, đơn vị.

b) Sử dụng phần mềm phòng chống vi rút (virus) máy tính trên tất cả máy chủ và máy trạm; phần mềm bản quyền trên các thiết bị mạng; phần mềm bản quyền các máy chủ, phần mềm bản quyền các nghiệp vụ chuyên ngành.

c) Trong trường hợp đơn vị có đội ngũ cán bộ kỹ thuật tốt khuyến khích đơn vị sử dụng và phát triển các phần mềm nguồn mở để giảm chi phí mua phần mềm bản quyền. Tuy nhiên, yêu cầu việc sử dụng phần mềm nguồn mở cũng phải đảm bảo tính an toàn, an ninh thông tin cho hệ thống mạng.

3. Hệ thống thông tin tại cơ quan, đơn vị phải được triển khai chức năng giám sát truy cập từ bên ngoài vào hệ thống, và từ hệ thống ra môi trường mạng bên ngoài *(ghi log)* để phục vụ cho công tác khắc phục sự cố, điều tra, phân tích và làm rõ các nguy cơ gây mất an toàn, an ninh thông tin, chức năng giới hạn truy cập website không phù hợp quy định hiện hành và gây nguy hiểm cho hệ thống thông tin.

4. Hệ thống mạng không dây (wireless) của các cơ quan, đơn vị phải được đặt mật khẩu (password) khi truy cập.

5. Mạng riêng ảo (VPN), các giải pháp truy cập từ xa về hệ thống thông tin của các cơ quan phải được bảo mật, quản lý kiểm soát các kết nối chặt chẽ, hủy bỏ các kết nối khi không còn sử dụng.

6. Tất cả các tài khoản truy cập vào hệ thống máy chủ, thiết bị mạng, máy tính, các ứng dụng phải được đặt mật khẩu (password), mật khẩu phải được đặt ở mức bảo mật cao (số lượng ký tự và nội dung mật khẩu), mật khẩu nên thường xuyên thay đổi, danh sách tài

khoản phải được quản lý, kiểm tra và cập nhật kịp thời, quyền truy cập của tài khoản phải được thiết lập phù hợp cho từng đối tượng.

Điều 5. Công việc của cán bộ chuyên trách về công nghệ thông tin của cơ quan, đơn vị trong lĩnh vực an toàn, an ninh thông tin

1. Tham gia các lớp đào tạo, bồi dưỡng, học tập, nghiên cứu, tiếp thu kiến thức, kỹ thuật và công nghệ đối với lĩnh vực an toàn, an ninh thông tin.

2. Quản lý chặt chẽ việc di chuyển trang thiết bị công nghệ thông tin lưu trữ các thông tin thuộc danh mục bí mật nhà nước.

3. Thực hiện cấp phát, thu hồi, cập nhật và quản lý tất cả các tài khoản truy cập vào hệ thống thông tin của đơn vị, hướng dẫn người sử dụng thay đổi mật khẩu ngay đầu tiên đăng nhập vào hệ thống, bảo vệ thông tin tài khoản theo quy định.

4. Triển khai áp dụng các giải pháp tổng thể đảm bảo an toàn, an ninh thông tin trong toàn hệ thống, triển khai các giải pháp kỹ thuật phòng chống virus máy tính, các mã độc hại, thư rác (spam mail) cho hệ thống và máy tính, kiểm soát và có giải pháp kỹ thuật chống truy cập trái phép vào hệ thống thông tin.

5. Thường xuyên cập nhật các bản vá lỗi hệ thống, cập nhật các phiên bản mới nhất đối với chương trình phòng chống virus máy tính

6. Cấu hình hệ thống với những chính sách bảo mật phù hợp hoạt động của hệ thống thông tin của đơn vị, đồng thời xác định các chức năng, cổng giao tiếp (port), giao thức (protocol) và dịch vụ (service) mạng không cần thiết để cấm và hạn chế sử dụng.

7. Thường xuyên sao lưu dữ liệu theo quy định, thường xuyên kiểm tra dữ liệu sao lưu phải đảm bảo tính sẵn sàng và toàn vẹn.

8. Sử dụng công cụ (Tool) hỗ trợ để kiểm tra, giám sát dữ liệu, thông tin từ bên trong hệ thống thông tin gửi ra bên ngoài khi cần thiết.

9. Thực hiện thu hồi và vô hiệu hóa tất cả các tài khoản, thiết bị dùng để truy cập vào hệ thống thông tin của cán bộ, công chức, viên chức ngay sau khi không còn làm việc tại cơ quan, đơn vị.

10. Thường xuyên thực hiện phân tích, đánh giá và báo cáo các rủi ro và nguy cơ gây mất an ninh, an toàn thông tin đối với hệ thống thông tin của cơ quan, đơn vị, nguyên nhân gây ra các rủi ro và nguy cơ gây mất an toàn, an ninh thông tin bao gồm:

a) Hiện tượng tự nhiên (nhiệt độ, không khí, mưa bão, sét....).

b) Truy cập trái phép vào hệ thống thông tin.

c) Do virus máy tính.

d) Cố ý làm thay đổi các thông số cấu hình hệ thống và phá hủy dữ liệu.

11. Tham mưu cho lãnh đạo cơ quan, đơn vị xây dựng các phương án hạn chế khắc phục các nguy cơ và rủi ro xảy ra mất an toàn, an ninh thông tin.

Điều 6. Giải quyết và khắc phục sự cố về an toàn, an ninh thông tin

1. Đối với người sử dụng

a) Thông tin, báo cáo kịp thời cho cán bộ chuyên trách về công nghệ thông tin của cơ quan, đơn vị khi phát hiện các sự cố gây mất an toàn, an ninh thông tin trong quá trình tham gia vào hệ thống thông tin của cơ quan, đơn vị.

b) Phối hợp tích cực trong quá trình giải quyết và khắc phục sự cố an toàn, an ninh thông tin.

2. Đối với cán bộ chuyên trách về công nghệ thông tin của các cơ quan, đơn vị

a) Lập biên bản ghi nhận sự cố gấy mất an toàn, an ninh thông tin đối với hệ thống thông tin của cơ quan, đơn vị, đồng thời thu thập các chứng cứ, dấu vết và nguyên nhân gây ra sự cố gây mất an toàn, an ninh thông tin.

b) Khẩn trương triển khai các biện pháp kỹ thuật để giải quyết và khắc phục sự cố, đồng thời báo cáo sự cố và kết quả khắc phục sự cố cho lãnh đạo cơ quan, đơn vị.

c) Trong trường hợp sự cố xảy ra ngoài khả năng giải quyết của cơ quan, đơn vị phải báo khẩn cấp về Sở Thông tin và Truyền thông Tỉnh, Trung tâm Ứng cứu Khẩn cấp máy tính Việt Nam (VNCERT) để được hỗ trợ, hướng dẫn và phối hợp khắc phục sự cố. Đồng thời tham mưu văn bản báo cáo sự cố về Sở Thông tin và Truyền thông, Công an Tỉnh.

3. Sở Thông tin và Truyền thông

a) Yêu cầu ngưng hoạt động một phần hoặc toàn bộ hệ thống các hệ thống thông tin của các cơ quan, đơn vị nhằm phục vụ công tác khắc phục sự cố về an toàn, an ninh thông tin.

b) Phối hợp với Công an Tỉnh trong điều tra làm rõ các nguyên nhân gây ra sự cố mất an toàn, an ninh thông tin khi có sự chỉ đạo của Ủy ban nhân dân Tỉnh

c) Phối hợp với Trung tâm Ứng cứu Khẩn cấp máy tính Việt Nam (VNCERT) khắc phục các sự cố gây mất an toàn, an ninh thông tin trên địa bàn Tỉnh.

d) Trong trường hợp sự cố xảy ra trên phạm vi rộng, ảnh hưởng và liên quan đến nhiều lĩnh vực quản lý nhà nước phải thông báo khẩn cấp và xin ý kiến chỉ đạo của Ủy ban nhân dân Tỉnh, Bộ Thông tin và Truyền thông.

Chương III

TRÁCH NHIỆM ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

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

1. Thủ trưởng các cơ quan, đơn vị chịu trách nhiệm trước Ủy ban nhân dân Tỉnh trong công tác đảm bảo an toàn, an ninh thông tin đối với hệ thống thông tin của cơ quan, đơn vị mình.

2. Trong phạm vi quản lý của mình, thủ trưởng các cơ quan, đơn vị có trách nhiệm:

a) Thực hiện và chỉ đạo cán bộ, công chức viên chức thuộc thẩm quyền quản lý thực hiện nghiêm túc quy định này.

b) Tạo điều kiện thuận lợi cho cán bộ, công chức, viên chức chuyên trách về công nghệ thông tin được đào tạo, bồi dưỡng chuyên môn trong lĩnh vực an toàn, an ninh thông tin.

c) Quan tâm đầu tư các thiết bị phần cứng, phần mềm liên quan đến công tác đảm bảo an toàn, an ninh thông tin.

d) Khi có sự cố hoặc nguy cơ mất an toàn, an ninh thông tin phải chỉ đạo khắc phục sự cố kịp thời, hạn chế thấp nhất mức thiệt hại có thể xảy ra, ưu tiên sử dụng lực lượng kỹ thuật tại chỗ của cơ quan, đơn vị mình, đồng thời lập biên bản và báo cáo bằng văn bản cho cơ quan có liên quan.

đ) Tạo điều kiện thuận lợi cho các cơ quan chức năng trong công tác điều tra, làm rõ nguyên nhân gây ra sự cố, lực lượng kỹ thuật tham gia khắc phục sự cố phải thực hiện theo đúng hướng dẫn chuyên môn của các cơ quan chức năng.

Điều 8. Trách nhiệm của Sở Thông tin và Truyền thông

1. Thực hiện công tác tham mưu cho Ủy ban nhân dân Tỉnh ban hành:

a) Văn bản chỉ đạo, kế hoạch nhằm đảm bảo an toàn, an ninh thông tin

b) Thành lập đoàn kiểm tra về đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin trong các cơ quan đơn vị nhà nước trên địa bàn Tỉnh

2. Hàng năm, tổ chức các lớp đạo tạo về an toàn, an ninh thông tin cho cán bộ chuyên trách công nghệ thông tin (Quản trị mạng) của các cơ quan, đơn vị.

3. Thực hiện nhiệm vụ cảnh báo về các nguy cơ, sự cố gây mất an toàn, an ninh thông tin.

4. Phối hợp với Trung tâm Ứng cứu Khẩn cấp máy tính Việt Nam (VNCERT) và các đơn vị liên quan trong thực hiện nhiệm vụ đảm bảo an toàn, an ninh thông tin.

5.Phối hợp với Công an Tỉnh và các cơ quan, đơn vị có liên quan tổ chức đoàn kiểm tra về an toàn, an ninh thông tin để kịp thời phát hiện xử lý các hành vi vi phạm theo thẩm quyền quy định.

6. Tổng hợp báo cáo và thông báo về tình hình an toàn, an ninh thông tin cho Ủy ban nhân dân Tỉnh và các cơ quan, đơn vị liên quan theo yêu cầu

Điều 9. Trách nhiệm Công an Tỉnh

1. Chủ trì, phối hợp với Sở Thông tin và Truyền thông và các cơ quan, đơn vị có liên quan kiểm soát, quản lý, phòng ngừa đấu tranh, ngăn chặn các loại tội phạm

lợi dụng hệ thống thông tin gây phương hại đến an toàn, an ninh thông tin và trật tự an toàn xã hội.

2. Phối hợp các cơ quan chức năng trong trao đổi, kiểm tra, đảm bảo an toàn an ninh thông tin.

3. Tăng cường 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 về lĩnh vực 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 trong lĩnh vực công nghệ thông tin.

Điều 10. Trách nhiệm của cán bộ, công chức và viên chức

1. Trách nhiệm của cán bộ chuyên trách công nghệ thông tin tại cơ quan, đơn vị:

a) Chịu trách nhiệm triển khai các biện pháp quản lý vận hành, quản lý kỹ thuật và tham mưu xây dựng các quy định về đảm bảo an toàn, an ninh thông tin cho toàn bộ hệ thống thông tin của cơ quan, đơn vị mình theo đúng nội dung của Hướng dẫn này.

b) Chủ động phối hợp với cán bộ, công chức và viên chức, cơ quan, đơn vị có liên quan trong việc kiểm tra, phát hiện và khắc phục sự cố về an toàn, an ninh thông tin.

c) Tuân thủ hướng dẫn kỹ thuật của các cơ quan, đơn vị chức năng trong các quá trình khắc phục sự cố về an toàn, an ninh thông tin.

2. Trách nhiệm của cán bộ, công chức, viên chức và người lao động tham gia sử dụng và khai thác hệ thống thông tin tại đơn vị.

a) Nghiêm túc thực hiện nội quy, quy định, quy trình nội bộ về đảm bảo an toàn, an ninh thông tin của cơ quan, đơn vị cũng như các quy định khác của pháp luật về nội dung này.

b) Khi phát hiện nguy cơ hoặc sự cố mất an toàn, an ninh thông tin phải báo cáo kịp thời cho cán bộ chuyên trách công nghệ thông tin của cơ quan, đơn vị mình để kịp thời ngăn chặn và xử lý.

c) Nâng cao ý thức cảnh giác và trách nhiệm về an toàn, an ninh thông tin.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 11. Tổ chức thực hiện

Lãnh đạo các cơ quan, đơn vị tổ chức triển khai thực hiện nghiêm túc Hướng dẫn này. Trong quá trình thực hiện, khi có khó khăn, vướng mắc, phát sinh cần sửa đổi, bổ sung, đề nghị cơ quan, đơn vị báo cáo kịp thời về Sở Thông tin và Truyền thông tổng hợp trình Ủy ban nhân dân Tỉnh xem xét và quyết định.

Sở Thông tin và Truyền thông phối hợp với Công an Tỉnh và các đơn vị có liên quan tiến hành kiểm tra định kỳ hàng năm và kiểm tra đột xuất các cơ quan, đơn vị có dấu hiệu vi phạm an toàn, an ninh thông tin.

Điều 12. Xử lý vi phạm

Tổ chức, cá nhân có hành vi vi phạm Hướng dẫn này tùy theo tính chất mức độ vi phạm sẽ bị xử lý kỷ luật theo trách nhiệm, xử phạt hành chính, bồi thường thiệt hại theo quy định của pháp luật.

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Lê Thanh Dũng