BỘ THÔNG TIN VÀ TRUYỀN THÔNG

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

Hà Nội, ngày 15 tháng 8 năm 2013

PHIẾU GIẢI QUYẾT VĂN BẢN ĐẾN

1. Tóm tắt nội dung văn bản:

- Số ký hiệu văn bản	: 22/2013/QĐ-UBND	Mức độ khẩn: Thường
- Số đến	: 9366	
- Ngày, tháng văn bản	: 08/08/13	
- Cơ quan ban hành	: UBND Tỉnh Bến Tre	
- Trích yếu	: Quyết định ban hành Quy chế đảm bảo an toàn, an ninh thông tin trên môi trường mạng trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Bến Tre	
- Thời hạn xử lý	:	

2. Ý kiến của lãnh đạo Văn phòng:

B/cáo: A. Hồng – Thứ trưởng

20/8

3. Ý kiến chỉ đạo của lãnh đạo Bộ:

Kính các đ/c CBQL
→ Cục Ứng cứu, VNCERT.
VP, CNTT, TTTT 28
15/8/2013

16/8/2013

19/08/13

20.8.13

4. Ý kiến chỉ đạo của Lãnh đạo đơn vị:

23.8

21/8

ỦY BAN NHÂN DÂN TỈNH BẾN TRE	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 22 /2013/QĐ-UBND	*Bến Tre, ngày 08 tháng 8 năm 2013*

QUYẾT ĐỊNH

Ban hành Quy chế đảm bảo an toàn, an ninh thông tin trên môi trường mạng trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Bến Tre

ỦY BAN NHÂN DÂN TỈNH BẾN TRE

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 và Ủy ban nhân dân ngày 03 tháng 12 năm 2004;

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 quy định về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

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;

Xét đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Tờ trình số 540/TTr-STTTT ngày 30 tháng 7 năm 2013,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế đảm bảo an toàn, an ninh thông tin trên môi trường mạng trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Bến Tre.

Điều 2. Các ông (bà): Chánh Văn phòng Ủy ban nhân dân tỉnh, Giám đốc Sở Thông tin và Truyền thông, Thủ trưởng các sở, ban, ngành tỉnh, Chủ

tịch Ủy ban nhân dân các huyện, thành phố, Chủ tịch Ủy ban nhân dân các xã, phường, thị trấn chịu trách nhiệm thi hành Quyết định này.

Quyết định này có hiệu lực sau 10 ngày kể từ ngày ký./.

Nơi nhận:
- Bộ Thông tin và Truyền thông;
- Website Chính phủ;
- Cục kiểm tra văn bản - BTP (để kiểm tra);
- TT.TU, TT HĐND tỉnh (thay báo cáo);
- Đoàn đại biểu Quốc hội tỉnh;
- Chủ tịch, các PCT UBND tỉnh;
- Sở Tư pháp (tự kiểm tra);
- Các sở, ban ngành tỉnh (để thực hiện);
- UBND các huyện, thành phố (để thực hiện);
- Báo Đồng Khởi (để đăng tin),
- Đài PT và TH tỉnh (để đưa tin);
- Chánh, PCVPNC Nguyễn Văn Dũng (để biết);
- Website tỉnh;
- Trung tâm Công báo tỉnh (2b);
- Phòng Tiếp dân (để niêm yết);
- Phòng NC: VHXH, TH;
- Lưu: VT.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Võ Thành Hạo

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

QUY CHẾ

Về việc đảm bảo an toàn, an ninh thông tin trên môi trường mạng trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Bến Tre

(Ban hành kèm theo Quyết định số 22 /2013/QĐ-UBND ngày 08 tháng 8 năm 2013 của Ủy ban nhân dân tỉnh Bến Tre)

Chương I

QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định các nội dung đảm bảo an toàn, an ninh thông tin trên môi trường mạng trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Bến Tre, bao gồm: công tác xây dựng các quy định quản lý đảm bảo an toàn, an ninh thông tin; việc áp dụng các biện pháp quản lý kỹ thuật, quản lý vận hành đảm bảo an toàn, an ninh thông tin đối với hệ thống thông tin.

Điều 2. Đối tượng áp dụng

1. Quy chế này được áp dụng đối với các cơ quan nhà nước trên địa bàn tỉnh Bến Tre, bao gồm: các sở, ban, ngành thuộc Ủy ban nhân dân tỉnh; Ủy ban nhân dân các huyện, thành phố, Ủy ban nhân dân các xã, phường, thị trấn (sau đây gọi tắt là cơ quan, đơn vị).

2. Cán bộ, công chức, viên chức đang làm việc 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 hệ thống thông tin tại các cơ quan, đơn vị.

Điều 3. Mục đích đảm bảo an toàn, an ninh thông tin

1. Giảm thiểu các nguy cơ gây sự cố mất an toàn thông tin và đảm bảo an ninh thông tin trong quá trình tác nghiệp của cán bộ, công chức.

2. Công tác đảm bảo an toàn, an ninh thông tin, bảo mật trên môi trường mạng là nhiệm vụ trọng tâm để đảm bảo thành công trong việc ứng dụng công nghệ thông tin trong hoạt động của các cơ quan nhà nước

Điều 4. 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 chống lại các nguy cơ tự nhiên, các hành động truy cập, sử dụng, phát tán, phá hoại, sửa đổi và phá hủy bất hợp pháp nhằm bảo đảm 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 thập, tạo, 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. Log File: Là một tập tin được tạo ra bởi một máy chủ web hoặc máy chủ proxy có chứa tất cả thông tin về các hoạt động trên máy chủ đó.

8. Firewall: là rào chắn (phần cứng, phần mềm) được lập ra nhằm kiểm soát người dùng mạng Internet truy nhập vào các thông tin không mong muốn và người dùng từ bên ngoài truy nhập trái phép thông tin trong mạng nội bộ.

9. Môi trường mạng bao gồm: mạng nội bộ (LAN); mạng diện rộng của Ủy ban nhân dân tỉnh, của ngành (WAN); mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước; mạng riêng ảo (VPN), mạng Intranet; mạng Internet.

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

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

Chương II

QUY ĐỊNH ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 5. Điều kiện đảm bảo thực hiện nhiệm vụ 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 trước khi tham gia sử dụng hệ thống thông tin.

2. Các cơ quan, đơn vị bố trí cán bộ 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. Xác định và ưu tiên phân bổ kinh phí cần thiết 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 hệ thống máy chủ, máy trạm và các công tác khác liên quan đến việc bảo đảm 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 đảm bảo an toàn, an ninh thông tin.

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

a) Mục tiêu, phạm vi và đối tượng áp dụng.

b) Quy định cụ thể quyền và trách nhiệm của từng đối tượng: lãnh đạo đơn vị, lãnh đạo cấp phòng, cán bộ chuyên trách về công nghệ thông tin và 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 phải đảm bảo chặt chẽ, đúng quy định.

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

h) Tổ chức thực hiện.

Điều 6. Trang thiết bị và hạ tầng công nghệ thông tin

1. Phòng máy chủ

Phòng máy chủ của các cơ quan phải độc lập, bộ phận chuyên trách hay cán bộ chuyên trách công nghệ thông tin trực tiếp quản lý, các cán bộ không liên quan không được vào phòng máy chủ. Phòng máy chủ phải đảm bảo khô, thoáng, nguồn điện cung cấp đảm bảo tính ổn định cao. Phòng máy chủ phải được trang bị máy lạnh và vận hành liên tục. Tùy theo điều kiện của từng cơ

quan mà bố trí phòng máy chủ riêng hoặc có thể ghép chung với bộ phận khác nhưng vẫn đảm bảo máy chủ hoạt động ổn định và vận hành liên tục

2. Máy chủ

Cấu hình máy chủ phải đủ mạnh để đáp ứng công việc. Máy chủ của các cơ quan chỉ dùng để triển khai phần mềm hệ thống, cài đặt phần mềm dùng chung, các cơ sở dữ liệu cần thiết và các phần mềm chống virus, ngoài ra không được cài thêm bất cứ phần mềm khác.

3. Thiết bị chống sét, phòng cháy, chữa cháy

Các cơ quan phải lắp đặt thiết bị chống sét, trang bị thiết bị phòng cháy, chữa cháy để bảo vệ các hệ thống công nghệ thông tin.

4. Thiết bị chuyển mạch

Thiết bị chuyển mạch mạng tin học của các cơ quan phải đảm bảo khả năng cung cấp các chức năng quản trị nhằm tăng cường độ an toàn và bảo mật cho hệ thống mạng như: cung cấp khả năng từ chối các kết nối không mong muốn hay trái phép vào hệ thống và khống chế số lượng kết nối vào hệ thống mạng nội bộ thông qua thiết bị chuyển mạch. Phải có ít nhất 01 thiết bị chuyển mạch hỗ trợ định tuyến IP cho mỗi mạng nội bộ, hỗ trợ chức năng điều khiển truy cập, chức năng xác thực thiết bị, xác thực người sử dụng và chức năng bảo mật quản trị mạng.

5. Tường lửa (Firewall)

Các cơ quan phải xây dựng tường lửa đảm bảo các yêu cầu gồm khả năng xử lý được số lượng kết nối đồng thời cao và chịu được thông lượng cao, hỗ trợ các công nghệ mạng riêng ảo thông dụng và có phần cứng mã hóa tích hợp để tăng khả năng mã hóa dữ liệu, cung cấp đầy đủ các cơ chế bảo mật cơ bản, quản lý luồng dữ liệu ra, vào và có khả năng bảo vệ hệ thống trước các loại tấn công từ chối dịch vụ.

Điều 7. Quy định về quản trị phần mềm

Trong quá trình đầu tư, thiết kế, xây dựng, nâng cấp các phần mềm hệ thống, các phần mềm ứng dụng dùng chung trong các cơ quan nhà nước phải đáp ứng yêu cầu quản trị, vận hành đảm bảo an toàn, an ninh thông tin.

1. Quản lý tài nguyên: cán bộ quản trị mạng có trách nhiệm kiểm tra, giám sát chức năng chia sẻ thông tin; tổ chức cấp phát tài nguyên trên máy chủ theo danh mục thư mục cho từng phòng/ ban; khuyến cáo người dùng cân nhắc việc chia sẻ tài nguyên cục bộ trên máy đang sử dụng, tuyệt đối không được chia sẻ toàn bộ ổ cứng. Khi thực hiện chia sẻ tài nguyên trên máy chủ hoặc trên máy cục bộ phải sử dụng mật khẩu để bảo vệ thông tin.

2. Quản lý đăng nhập hệ thống: các hệ thống thông tin cần giới hạn số lần đăng nhập vào hệ thống. Hệ thống tự động khóa tài khoản hoặc cô lập tài khoản khi liên tục đăng nhập sai vượt quá số lần quy định. Tổ chức theo dõi,

giám sát tất cả các phương tiện đăng nhập từ xa; yêu cầu người sử dụng đặt mật khẩu với độ an toàn cao, giám sát, nhắc nhở, khuyến cáo nên thay đổi mật khẩu thường xuyên.

3. Quản lý tài khoản: Các tài khoản và định danh người dùng trong các hệ thống thông tin, bao gồm: tạo mới, kích hoạt, sửa đổi và loại bỏ các tài khoản, đồng thời tổ chức kiểm tra các tài khoản của hệ thống thông tin ít nhất 6 tháng/lần thông qua các công cụ của hệ thống. Hủy tài khoản, quyền truy cập hệ thống đối với cán bộ, công chức đã chuyển công tác hoặc thôi việc.

4. Quản lý nhật ký (log file): Hệ thống thông tin phải ghi nhận các sự kiện như: quá trình đăng nhập vào hệ thống, các thao tác cấu hình hệ thống. Thường xuyên kiểm tra, sao lưu các log file theo từng tháng để lưu vết theo dõi, xác định những sự kiện đã xảy ra của hệ thống và hạn chế việc tràn log file gây ảnh ưởng đến hoạt động của hệ thống

5. Phòng chống mã độc, virus: Trên các máy chủ, các thiết bị di động trong mạng và hệ thống thông tin phải cài đặt phần mềm chống virus, thư rác phù hợp để phát hiện, loại trừ mã độc, virus và cài đặt các phần mềm này trên máy trạm.

6. Quản lý cài đặt: cán bộ, công chức, viên chức không được tự ý cài đặt thêm chương trình khác trên máy tính cá nhân nhằm tránh sự lây lan của virus, gây xung đột phần mềm.

Điều 8. Bảo vệ bí mật nhà nước trong hoạt động ứng dụng công nghệ thông tin

1. Quy định về soạn thảo, in ấn, phát hành và sao chụp tài liệu mật

a) Không được sử dụng máy tính nối mạng internet để soạn thảo văn bản, chuyển giao, lưu trữ thông tin có nội dung thuộc bí mật nhà nước; cung cấp tin, tài liệu và đưa thông tin bí mật nhà nước trên cổng/trang thông tin điện tử.

b) Không được in, sao chụp tài liệu bí mật nhà nước trên các thiết bị kết nối mạng internet.

2. Khi sửa chữa, khắc phục các sự cố của máy tính dùng soạn thảo văn bản mật, các cơ quan phải báo cáo cho cơ quan có thẩm quyền. Không được cho phép các công ty tư nhân hoặc người không có trách nhiệm trực tiếp sửa chữa, xử lý, khắc phục sự cố.

3. Trước khi thanh lý các máy tính trong các cơ quan nhà nước, cán bộ chuyên trách công nghệ thông tin phải dùng các biện pháp kỹ thuật xóa bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính.

Điều 9. Quản lý, vận hành hệ thống thông tin của đơn vị

1. Hệ thống thông tin của các cơ quan, đơn vị phải có cơ chế sao lưu dữ liệu ở mức hệ thống, dữ liệu của các ứng dụng, dữ liệu của người sử dụng; cơ chế sao lưu dữ liệu phải được thực hiện thường xuyên; thiết bị lưu trữ dữ liệu

được sao lưu 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, an toàn thông tin bằng các thiết bị phần cứng và phần mềm phù hợp với quy mô của đơn vị.

3. Hệ thống thông tin của đơn vị phải được triển khai chức năng giám sát truy cập từ ngoài vào hệ thống, từ hệ thống gửi ra bên ngoài; ghi lại nhật ký (log file) ra, vào hệ thống để phục vụ công tác khắc phục sự cố, điều tra, phân tích và làm rõ các nguy cơ gây ra mất an toàn, an ninh thông tin; chức năng không cho người dùng truy cập một số website không phù hợp với quy định hiện hành.

4. Hệ thống mạng không dây (wireless) của các cơ quan, đơn vị phải được thiết lập khóa khi truy cập.

5. Mạng riêng ảo (VPN) của các cơ quan, đơn vị kết nối để truy cập vào hệ thống thông tin phải được bảo mật; quản lý và kiểm soát chặt chẽ các kết nối; hủy bỏ 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 thiết lập mật khẩu; mật khẩu phải được đặt ở mức bảo mật cao (số lượng ký tự và nội dung của mật khẩu); mật khẩu phải thường xuyên thay đổi với tần suất phù hợp; 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 10. Cán bộ chuyên trách về công nghệ thông tin của đơn vị

1. Được đảm bảo điều kiện về đào tạo, bồi dưỡng, học tập, nghiên cứu, tiếp thu kiến thức, kỹ thuật và công nghệ mới đối với lĩnh vực an toàn, an ninh thông tin.

2. Quản lý chặt chẽ việc di chuyển các 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 sau khi đăng nhập lần đầu tiên; bảo vệ thông tin của 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, mã độc hại, thư rác cho hệ thống và máy tính cá nhân; 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 đối với hệ thống, cập nhật các phiên bản mới đối với chương trình chống virus.

6. Thường xuyên sao lưu dữ liệu theo quy định; kiểm tra dữ liệu sao lưu phải đảm bảo tính sẵn sàng, tin cậy và toàn vẹn.

7. Thường xuyên thực hiện phân tích, đánh giá và báo cáo các rủi ro và nguy cơ gây mất an toàn, an ninh thông tin đối với hệ thống thông tin của đơn vị; nguyên nhân gây ra các rủi ro và nguy cơ gây mất an toàn, an ninh thông tin bao gồm: hiện tượng tự nhiên (nhiệt độ, không khí, mưa bão, sét), truy cập trái phép, virus, cố ý làm thay đổi thông số cấu hình hệ thống và phá hủy dữ liệu. Đồng thời tham mưu và xây dựng phương án hạn chế, khắc phục các rủi ro và nguy cơ có thể xảy ra.

Điều 11. Giải quyết và khắc phục sự cố 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 đơn vị.

b) Phối hợp tích cực trong suốt quá trình giải quyết và khắc phục sự cố.

2. Đối với cán bộ chuyên trách về công nghệ thông tin

a) Xử lý khẩn cấp: Khi phát hiện hệ thống bị tấn công, thông qua các dấu hiệu như luồng tin (traffic) tăng lên bất ngờ, nội dung bị thay đổi, hệ thống hoạt động chậm bất thường cần thực hiện các bước cơ bản sau:

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

Bước 2: Sao chép nhật ký (log file) và toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ;

Bước 3: Khôi phục lại hệ thống bằng cách chuyển dữ liệu sao lưu mới nhất để hệ thống hoạt động trở lại bình thường.

Lập biên bản ghi nhận sự cố gây ra 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 (nếu có); đồng thời báo cáo sự cố và kết quả khắc phục sự cố cho Thủ trưởng cơ quan, đơn vị.

b) Trong trường hợp sự cố xảy ra ngoài khả năng giải quyết của cơ quan, đơn vị phải báo cáo khẩn cấp bằng điện thoại, gửi thư điện tử cho Sở Thông tin và Truyền thông để được hỗ trợ, hướng dẫn và phối hợp khắc phục sự cố; đồng thời tham mưu văn bản báo cáo sự cố gửi Sở Thông tin và Truyền thông, Công an tỉnh và các đơn vị có liên quan.

3. Sở Thông tin và Truyền thông

a) Quyết định toàn diện về mặt kỹ thuật đối với các cơ quan, đơn vị trong quá trình khắc phục sự cố về an toàn, an ninh thông tin.

b) Chỉ đạo các đơn vị trực thuộc nhanh chóng hỗ trợ, phối hợp và hướng dẫn các cơ quan, đơn vị khắc phục sự cố mất an toàn, an ninh thông tin.

c) Yêu cầu ngưng hoạt động một phần hoặc toàn bộ 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.

d) 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.

đ) Trong trường hợp sự cố xảy ra có phạm vi rộng, ảnh hưởng và liên quan đến nhiều ngành, nhiều lĩnh vực 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 12. 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 toàn bộ hệ thống thông tin của đơn vị mình.

2. Thực hiện và chỉ đạo cán bộ, công chức thuộc thẩm quyền quản lý thực hiện nghiêm túc Quy định này.

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

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

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

6. 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 thực hiện đúng theo hướng dẫn chuyên môn của Sở Thông tin và Truyền thông.

Điều 13. Trách nhiệm của Sở Thông tin và Truyền thông

1. Chịu trách nhiệm toàn diện trước Ủy ban nhân dân tỉnh về công tác đảm bảo an toàn, an ninh thông tin trong hoạt động ứng công nghệ thông tin của các cơ quan nhà nước trên phạm vi toàn tỉnh.

2. Thực hiện công tác tham mưu Ủy ban nhân dân tỉnh ban hành:

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

b) Xây dựng tiêu chuẩn đánh giá mức độ an toàn, an ninh thông tin đối với hệ thống thông tin của các đơn vị.

c) Thành lập Đoàn kiểm tra liên ngành về đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin trong các cơ quan nhà nước.

3. Hằng năm tổ chức đào tạo chuyên sâu về an toàn, an ninh thông tin cho lực lượng đảm bảo an toàn, an ninh thông tin của các cơ quan, đơn vị.

4. Thực hiện nhiệm vụ cảnh báo về nguy cơ hoặc sự cố mất an toàn, an ninh thông tin.

5. Tổ chức Hội nghị, Hội thảo chuyên đề về an toàn, an ninh thông tin.

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

7. 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.

8. Chủ động hướng dẫn các cơ quan, đơn vị xây dựng quy chế nội bộ, hỗ trợ kỹ thuật, nội dung, thời gian báo cáo công tác đảm bảo an toàn, an ninh thông tin.

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

Điều 14. 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 quản lý, kiểm soát, 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 trong cơ quan nhà nước.

2. Phối hợp với các cơ quan chức năng trong trao đổi, kiểm tra, 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 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 trên lĩnh vực công nghệ thông tin.

Điều 15. Trách nhiệm của cán bộ, công chức, viên chức tại các cơ quan, đơn vị

1. Trách nhiệm của cán bộ chuyên trách công nghệ thông tin

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 đơn vị mình đúng theo nội dung Quy định này.

b) Chủ động phối hợp với cá nhân, 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 theo sự hướng dẫn kỹ thuật của Sở Thông tin và Truyền thông trong quá trình khắc phục sự cố về an toàn, an ninh thông tin.

2. Trách nhiệm của cán bộ, công chức, viên chức tham gia sử dụng và khai thác hệ thống thông tin

a) Nghiêm túc thực hiện các nội quy, quy chế, quy trình nội bộ về đảm bảo an toàn, an ninh thông tin của 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 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

KIỂM TRA CÔNG TÁC ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 16. Kiểm tra định kỳ và đột xuất

1. Đoàn kiểm tra xây dựng kế hoạch và thực hiện kiểm tra định kỳ hàng năm về công tác đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước.

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

Điều 17. Trách nhiệm và phối hợp trong công tác kiểm tra

1. Đoàn kiểm tra có trách nhiệm thông báo thời gian, địa điểm, nội dung và thành phần cho đơn vị được kiểm tra biết trước ít nhất 05 ngày để chuẩn bị.

2. Đơn vị được kiểm tra:

a) Chuẩn bị nội dung báo cáo theo yêu cầu của Đoàn kiểm tra.

b) Có đại diện lãnh đạo và cán bộ chuyên trách công nghệ thông tin của đơn vị để cùng làm việc với Đoàn kiểm tra.

c) Tạo thuận lợi cho công tác kiểm tra.

Chương V

TỔ CHỨC THỰC HIỆN

Điều 18. Tổ chức thực hiện

1. Sở Thông tin và Truyền thông chủ trì, phối hợp với các cơ quan, đơn vị có liên quan triển khai thực hiện tốt nội dung Quy chế này.

2. Các cơ quan, đơn vị chủ động xây dựng, ban hành quy chế nội bộ về đảm bảo an toàn, an ninh thông tin phù hợp với Quy chế này. Định kỳ hàng năm báo cáo tổng hợp tình hình đảm bảo an toàn, an ninh thông tin tại đơn vị mình gửi Sở Thông tin và Truyền thông ***trước ngày 15 tháng 10*** để tổng hợp, báo cáo Ủy ban nhân dân tỉnh.

3. Thủ trưởng các cơ quan, đơn vị tổ chức triển khai thực hiện nghiêm túc Quy chế này. Trong quá trình thực hiện, nếu có khó khăn, vướng mắc, phát sinh cần sửa đổi, bổ sung, đề nghị các cơ quan, đơn vị kịp thời báo cáo về Sở Thông tin và Truyền thông để tổng hợp trình Ủy ban nhân dân tỉnh xem xét, quyết định./.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Võ Thành Hạo