ỦY BAN NHÂN DÂN TỈNH SÓC TRĂNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 10 /2013/QĐ-UBND	*Sóc Trăng, ngày 08 tháng 4 năm 2013*

QUYẾT ĐỊNH

Ban hành Quy chế 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 Sóc Trăng.

ỦY BAN NHÂN DÂN TỈNH SÓC TRĂNG

Căn cứ Luật Tổ chức Hội đồng nhân dân và Ủy ban nhân dân số 11/2003/QH11 ngày 26 tháng 11 năm 2003;

Căn cứ Luật Ban hành văn bản quy phạm pháp luật của Hội đồng nhân dân, Ủy ban nhân dân số 31/2004/QH11 ngày 03 tháng 12 năm 2004;

Căn cứ Luật Công nghệ thông tin số 67/2006/QH11 ngày 29 tháng 6 năm 2006;

Căn cứ Nghị định số 63/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ quy định xử phạt hành chính trong lĩnh vực công nghệ thông tin;

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ về việc ứng dụng công nghệ thông tin trong hoạt động cơ quan nhà nước;

Căn cứ Thông tư số 01/2011/TT-BTTTT ngày 04 tháng 01 năm 2011 của Bộ Thông tin và Truyền thông về công bố danh mục tiêu chuẩn về ứng dụng công nghệ thông tin trong cơ quan nhà nước;

Căn cứ Chỉ thị số 03/2007/CT-BBCVT ngày 23 tháng 02 năm 2007 của Bộ Bưu chính, viễn thông về việc tăng cường đảm bảo an ninh thông tin trên mạng Internet;

Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế 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 Sóc Trăng.

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

Điều 3. Chánh Văn phòng UBND tỉnh, Thủ trưởng các cơ quan nhà nước trực thuộc UBND tỉnh, Chủ tịch UBND các huyện, thị xã, thành phố trên địa bàn tỉnh Sóc Trăng và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- VPCP;
- Bộ TTTT;
- Cục KTVB-BTP;
- TT. TU, HĐND tỉnh;
- CT, các PCT UBND tỉnh;
- Lưu: VX, QT, CNTT, HC.

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

Quách Việt Tùng

ỦY BAN NHÂN DÂN
TỈNH SÓC TRĂNG

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

QUY CHẾ

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 Sóc Trăng .

(Kèm theo Quyết định số 10 /2013/QĐ-UBND ngày 08/4/2013 của Ủy ban nhân dân tỉnh Sóc Trăng)

Chương I
NHỮNG QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định các nội dung của công tác đảm bảo an toàn, an ninh thông tin, bảo mật trên môi trường mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước, đơn vị sự nghiệp trên địa bàn tỉnh Sóc Trăng, 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 thuộc tỉnh, bao gồm: các sở, ban ngành, đoàn thể và các đơn vị sự nghiệp trực thuộc Ủy ban nhân dân tỉnh; các phòng, ban và Ủy ban nhân dân các xã, phường, thị trấn thuộc Ủy ban nhân dân các huyện, thị xã, thành phố (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 tổ chức, cá nhân có liên quan áp dụng Quy chế này trong việc vận hành, khai thác và sử dụng hệ thống thông tin tại các cơ quan, đơn vị.

Điều 3. Mục đích đảm bảo an toàn, an ninh thông tin, bảo mật trên môi trường mạng

1. Giảm thiểu được các nguy cơ gây sự cố mất an toàn thông tin và đảm bảo an ninh thông tin trong quá trình tham gia hoạt động trên môi trường mạng.

2. Công tác đảm bảo an toàn, an ninh thông tin, bảo mật trên môi trường mạng là một trong những nhiệm vụ trọng tâm để đảm bảo thành công trong việc ứng dụng công nghệ thông tin trong các cơ quan, đơn vị.

Điều 4. Giải thích từ ngữ

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

1. *Tính tin cậy*: Đảm bảo thông tin chỉ có thể được truy nhập bởi những người được cấp quyền sử dụng.

2. *Tính toàn vẹn*: Bảo vệ sự chính xác và đầy đủ của thông tin và các phương pháp xử lý thông tin.

3. *Tính sẵn sàng*: Đảm bảo những người được cấp quyền có thể truy nhập thông tin vào các tài sản liên quan ngay khi có nhu cầu.

4. *Hệ thống thông tin*: Là một tập hợp và kết hợp của các phần cứng, phần mềm và các hệ 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 và tri thức nhằm phục vụ các mục tiêu của tổ chức.

5. *Đảm bảo an toàn, an ninh thông tin (ATANTT)*: Là việc bảo vệ thông tin số và các hệ thống thông tin chống lại các nguy cơ tự nhiên hoặc do con người gây ra nhằm đảm bảo cho 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 an toàn, an ninh thông tin bao gồm bảo vệ an toàn mạng và hạ tầng thông tin, an toàn máy tính, dữ liệu và các ứng dụng công nghệ thông tin.

6. *Cấu hình chuẩn*: Là cấu hình được các nhà sản xuất thiết bị, phần mềm, khuyến nghị áp dụng, nhằm loại bỏ các xung đột, lỗ hổng có thể xảy ra trong quá trình cấu hình thiết bị.

7. *Cổng giao tiếp (Port)*: Để định danh các ứng dụng gửi và nhận dữ liệu, mỗi ứng dụng sẽ tương ứng với một cổng giao tiếp, những ứng dụng phổ biến được đặt với số hiệu cổng định trước, nhằm định danh duy nhất các ứng dụng đó. Khi máy tính sử dụng dịch vụ nào thì cổng giao tiếp tương ứng với dịch vụ đó sẽ mở.

8. *Giao thức (Protocol)*: Là tập hợp các qui tắc, qui ước truyền thông của mạng mà tất cả các thực thể tham gia truyền thông phải tuân theo.

9. *Virus máy tính*: Là một chương trình hay một đoạn mã có khả năng tự sao chép chính nó từ đối tượng lây nhiễm này sang đối tượng khác với mục đích gây hại cho máy tính.

10. *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.

11. *TCVN 7562: 2005*: Tiêu chuẩn Việt Nam về mã thực hành quản lý ATANTT.

12. *ISO 17799:2005*: Tiêu chuẩn Quốc tế cung cấp các hướng dẫn quản lý an toàn bảo mật thông tin dựa trên quy phạm công nghiệp tốt nhất (tập quy phạm cho quản lý an toàn, bảo mật thông tin).

13. *ISO 27001: 2005*: Tiêu chuẩn Quốc tế về quản lý bảo mật thông tin do Tổ chức Chất lượng Quốc tế và Hội đồng Điện tử Quốc tế xuất bản vào tháng 10/2005.

Chương II
NỘI DUNG ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 5. Các biện pháp quản lý vận hành trong công tác an toàn, an ninh thông tin và bảo mật

1. Đối với các cơ quan, đơn vị:

a) Trang bị đầy đủ kiến thức bảo mật cơ bản cho cán bộ, công chức, viên chức trước khi cho phép truy nhập và sử dụng hệ thống thông tin;

b) Bố trí cán bộ, công chức, viên chức chuyên trách hoặc phụ trách về công nghệ thông tin (sau đây gọi là cán bộ chuyên trách). Cán bộ chuyên trách cần phải có các kiến thức về mạng và quản trị mạng máy tính; kiến thức về an toàn, an ninh thông tin trước khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ;

c) Cần hủy bỏ quyền truy nhập hệ thống thông tin, đảm bảo việc thu hồi lại tất cả các tài sản liên quan tới hệ thống thông tin (tài khoản, khóa, thẻ nhận dạng,...) đối với nhân viên đã chấm dứt hợp đồng hay nghỉ việc và đảm bảo khả năng vẫn truy nhập được vào các hồ sơ được tạo ra bởi nhân viên đó (phải bàn giao trước khi rời khỏi cơ quan, đơn vị);

d) Xác định và phân bổ kinh phí đầu tư cần thiết để bảo vệ hệ thống thông tin hoạt động tối ưu.

2. Đối với cán bộ chuyên trách tại các cơ quan, đơn vị:

a) Được Thủ trưởng cơ quan, đơn vị đảm bảo điều kiện học tập, tiếp thu công nghệ, kiến thức an toàn, an ninh và bảo mật thông tin;

b) Chịu trách nhiệm tham mưu chuyên môn và vận hành an toàn hệ thống thông tin của cơ quan, đơn vị theo nhiệm vụ được Thủ trưởng cơ quan, đơn vị phân công;

c) Thường xuyên cập nhật cấu hình chuẩn cho các thành phần của hệ thống thông tin, khi tiến hành cài đặt và thiết lập cấu hình cho các sản phẩm an toàn thông tin (phần cứng và phần mềm) nhưng vẫn phải duy trì yêu cầu hoạt động tốt của hệ thống thông tin, không bị gián đoạn;

d) Cấu hình hệ thống thông tin chỉ cung cấp những chức năng thiết yếu nhất; cấm, hạn chế sử dụng chức năng, cổng giao tiếp mạng, giao thức và các dịch vụ không cần thiết;

đ) Sao lưu thông tin ở mức người dùng và mức hệ thống (bao gồm trạng thái hệ thống thông tin) và lưu trữ thông tin sao lưu tại nơi an toàn. Đồng thời, tổ chức kiểm tra thông tin sao lưu để đảm bảo tính sẵn sàng và toàn vẹn thông tin;

e) Triển khai cơ chế chống virus, thư rác cho những hệ thống xung yếu hiện hữu (firewall, mail server,...) và tại các máy trạm, máy chủ, các thiết bị di động trong mạng. Tổ chức sử dụng cơ chế chống virus, thư rác để phát hiện và loại trừ những đoạn mã độc hại (virus, trojan, worms,...) được truyền tải bởi thư điện tử, tập tin đính kèm từ Internet, thiết bị lưu trữ di động để khai thác lỗ hổng của hệ thống thông tin. Đồng thời, cập nhật cơ chế chống virus, thư rác thường xuyên sao cho phù hợp với quy trình và chính sách quản lý cấu hình hệ thống thông tin của tổ chức. Cần cân nhắc việc sử dụng phần mềm chống virus từ nhiều hãng phân phối khác nhau;

g) Thực hiện việc đánh giá, báo cáo các rủi ro và mức độ nghiêm trọng các rủi ro đó. Các rủi ro đó có thể xảy ra do sự truy cập trái phép, sử dụng trái phép, mất, thay đổi hoặc phá hủy thông tin và hệ thống thông tin.

Điều 6. Các biện pháp quản lý kỹ thuật cho công tác an toàn, an ninh thông tin

1. Sơ đồ hệ thống mạng của cơ quan, đơn vị phải được bảo mật tuyệt đối theo quy định và ứng với từng chức năng vận hành của các máy chủ mà có cơ chế, chính sách bảo mật phù hợp riêng, tùy theo các dịch vụ hay ứng dụng như: Websites, hệ thống thư điện tử, hệ thống quản lý tên miền, cơ sở dữ liệu,... mà thiết lập các tường lửa thích hợp (phần cứng hoặc phần mềm) và chính sách an toàn, an ninh khác nhau theo từng vùng (như vùng Outside, DMZ, Inside và Managerment) nhằm đảm bảo an toàn, an ninh thông tin tốt nhất.

2. Đối với cán bộ chuyên trách chịu trách nhiệm trực và quản trị mạng luôn tuyệt đối tuân theo các quy định, quy trình và các quy chế về an toàn, an ninh thông tin mạng và theo các quy định hiện hành của nhà nước.

3. Các cơ quan, đơn vị tổ chức quản lý các tài khoản của hệ thống thông tin, bao gồm: Tạo mới, kích hoạt, sửa đổi, vô hiệu hóa và loại bỏ các tài khoản. Đồng thời, tổ chức kiểm tra các tài khoản của hệ thống thông tin ít nhất 01 lần/năm và triển khai các công cụ tự động để hỗ trợ việc quản lý các tài khoản của hệ thống thông tin.

4. Hệ thống thông tin phải giới hạn một số hữu hạn lần đăng nhập sai liên tiếp (tối đa 03 lần). Hệ thống tự động khóa tài khoản hoặc cô lập 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.

5. Tổ chức theo dõi và kiểm soát tất cả các phương pháp truy nhập từ xa tới hệ thống thông tin bao gồm cả sự truy nhập có chức năng đặc quyền. Hệ thống cần có quá trình kiểm tra, cho phép ứng với mỗi phương pháp truy nhập từ xa và chỉ cho phép những người thật sự cần thiết truy nhập từ xa vào. Đồng thời, tổ chức triển khai cơ chế tự động giám sát và điều khiển các truy nhập từ xa.

6. Cần thiết lập phương pháp hạn chế truy cập mạng không dây; giám sát và điều khiển truy nhập không dây. Tổ chức sử dụng chứng thực và mã hóa để bảo vệ truy nhập không dây tới hệ thống thông tin.

7. Hệ thống thông tin cần ghi nhận vào bản nhật ký ít nhất các sự kiện sau: Quá trình đăng nhập hệ thống, các thao tác cấu hình hệ thống và quá trình truy xuất hệ thống. Đồng thời, ghi nhận đầy đủ các thông tin trong các bản ghi nhật ký để xác định những sự kiện nào đã xảy ra, nguồn gốc và các kết quả của sự kiện để có cơ chế bảo vệ và lưu giữ nhật ký trong một khoảng thời gian nhất định.

Điều 7. Xây dựng quy chế nội bộ đảm bảo an toàn, an ninh thông tin

1. Các cơ quan, đơn vị phải ban hành quy chế nội bộ, đảm bảo quy định rõ các vấn đề sau:

a) Mục tiêu và phương hướng thực hiện công tác đảm bảo an toàn, an ninh cho hệ thống thông tin;

b) Nguyên tắc phân loại và quản lý mức độ ưu tiên đối với các tài nguyên của hệ thống thông tin (phần mềm, dữ liệu, trang thiết bị,...);

c) Quản lý phân quyền và trách nhiệm đối với từng cá nhân khi tham gia sử dụng hệ thống thông tin;

d) Quản lý và điều hành hệ thống máy chủ, thiết bị mạng, thiết bị bảo vệ mạng một cách an toàn;

đ) Kiểm tra, rà soát và khắc phục sự cố an toàn, an ninh của hệ thống thông tin sử dụng các biện pháp trong Điều 5 và Điều 6 của Quy chế;

e) Nguyên tắc chung sử dụng an toàn và hiệu quả đối với toàn bộ cá nhân tham gia sử dụng hệ thống thông tin;

g) Báo cáo tổng hợp tình hình an toàn, an ninh của hệ thống thông tin theo định kỳ.

2. Các cơ quan, đơn vị xây dựng quy chế an toàn, an ninh thông tin căn cứ các tiêu chuẩn kỹ thuật quản lý an toàn, an ninh thông tin theo bộ tiêu chuẩn TCVN 7562:2005 và ISO/IEC 17799:2005 tại Phụ lục I kèm theo Quy chế này để có sự lựa chọn áp dụng phù hợp.

Điều 8. Xây dựng và áp dụng quy trình đảm bảo an toàn, an ninh thông tin

1. Các cơ quan, đơn vị phải xây dựng và áp dụng quy trình đảm bảo an toàn, an ninh cho hệ thống thông tin nhằm giảm thiểu các nguy cơ gây sự cố, tạo điều kiện cho việc khắc phục và truy vết trong trường hợp có sự cố xảy ra. Nội dung của quy trình có thể chia làm các bước cơ bản như:

a) Lập kế hoạch bảo vệ an toàn, an ninh cho hệ thống thông tin;

b) Xây dựng hệ thống bảo vệ an toàn, an ninh thông tin;

c) Quản lý và vận hành hệ thống bảo vệ an toàn, an ninh thông tin;

d) Kiểm tra đánh giá hoạt động của hệ thống bảo vệ an toàn, an ninh thông tin;

đ) Bảo trì và nâng cấp hệ thống bảo vệ an toàn, an ninh thông tin.

2. Các cơ quan, đơn vị tham khảo các bước cơ bản để xây dựng khung quy trình đảm bảo an toàn, an ninh thông tin cho hệ thống thông tin tại Phụ lục II kèm theo Quy chế này và tiêu chuẩn Quốc tế ISO 27001:2005.

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 9. Trách nhiệm của các cơ quan, đơn vị

1. Thủ trưởng các cơ quan, đơn vị có trách nhiệm thực hiện các quy định tại Quy chế này và chịu trách nhiệm toàn diện trước UBND tỉnh trong công tác bảo vệ an toàn, an ninh thông tin của cơ quan, đơn vị phụ trách.

2. Khi có sự cố hoặc nguy cơ mất an toàn, an ninh thông tin kịp thời áp dụng mọi biện pháp để khắc phục và hạn chế thiệt hại, ưu tiên sử dụng lực lượng kỹ thuật về ATANTT của cơ quan, đơn vị và lập biên bản, báo cáo bằng văn bản cho cơ quan cấp trên quản lý trực tiếp và Sở Thông tin và Truyền thông. Trường

hợp có sự cố nghiêm trọng vượt quá khả năng khắc phục của cơ quan, đơn vị, phải báo cáo ngay cho cơ quan cấp trên quản lý trực tiếp và Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ.

3. Tạo điều kiện thuận lợi cho các cơ quan chức năng tham gia khắc phục sự cố và thực hiện đúng theo hướng dẫn.

4. Phối hợp với đoàn kiểm tra để việc triển khai công tác kiểm tra khắc phục sự cố diễn ra nhanh chóng và đạt hiệu quả; đồng thời cung cấp đầy đủ các thông tin khi đoàn kiểm tra yêu cầu.

5. Báo cáo tình hình và kết quả thực hiện công tác đảm bảo an toàn, an ninh thông tin tại cơ quan, đơn vị và gửi về Sở Thông tin và Truyền thông định kỳ hàng năm (trước ngày 15 tháng 12).

Điều 10. Trách nhiệm của cán bộ, công chức, viên chức trong các cơ quan, đơn vị

1. Nghiêm chỉnh thi hành các quy chế nội bộ, quy trình về ATANTT 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, an ninh thông tin tại cơ quan, đơn vị.

2. Khi phát hiện sự cố phải báo cáo ngay với cấp trên và bộ phận chuyên trách để kịp thời ngăn chặn, xử lý.

3. Hưởng ứng, tham gia các chương trình đào tạo, hội nghị về an toàn, an ninh thông tin do Sở Thông tin và Truyền thông và các cơ quan chức năng tổ chức.

Điều 11. Trách nhiệm của Sở Thông tin và Truyền thông

1. Tham mưu UBND tỉnh về công tác đảm bảo an toàn, an ninh thông tin trên địa bàn tỉnh và phối hợp với các cơ quan, đơn vị liên quan trong việc đảm bảo an toàn, an ninh cho các hệ thống thông tin cấp tỉnh.

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

3. Tùy theo mức độ sự cố, phối hợp Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) và các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố thông tin.

4. Hướng dẫn, giám sát các cơ quan, đơn vị xây dựng quy chế và thực hiện việc đảm bảo an toàn, an ninh cho hệ thống thông tin theo quy định của pháp luật.

Chương IV
CÔNG TÁC THANH TRA, KIỂM TRA AN TOÀN, AN NINH THÔNG TIN

Điều 12. Kế hoạch kiểm tra hàng năm

1. Sở Thông tin và Truyền thông chủ trì, phối hợp các cơ quan, đơn vị liên quan và Công an tỉnh kiểm tra an toàn, an ninh thông tin tại các cơ quan, đơn vị định kỳ hàng năm (tối thiểu 01 lần/năm).

2. Tiến hành kiểm tra đột xuất các cơ quan, đơn vị khi có dấu hiệu vi phạm an toàn, an ninh trong hệ thống thông tin.

Điều 13. Quan hệ phối hợp và trách nhiệm của các cơ quan chức năng liên quan

1. Sở Thông tin và Truyền thông:

a) Chịu trách nhiệm chủ trì, phối hợp với các cơ quan chức năng liên quan để thành lập Đoàn kiểm tra và triển khai, báo cáo công tác kiểm tra an toàn, an ninh thông tin trên quy mô toàn tỉnh;

b) Tổ chức xử lý các hành vi vi phạm an toàn, an ninh thông tin gây thiệt hại cho hệ thống thông tin thuộc các cơ quan, đơn vị trên địa bàn tỉnh theo thẩm quyền;

c) Tuyên truyền công tác an toàn, an ninh thông tin tại các cơ quan, đơn vị trên địa bàn tỉnh.

2. Trách nhiệm của Công an tỉnh:

a) Phối hợp Sở Thông tin và Truyền thông kiểm tra công tác an toàn, an ninh thông tin;

b) Điều tra và xử lý các trường hợp vi phạm an toàn, an ninh thông tin theo thẩm quyền.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 14. Điều khoản thi hành

Sở Thông tin và Truyền thông chủ trì, phối hợp với các cơ quan, đơn vị 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 báo cáo về Sở Thông tin và Truyền thông tổng hợp trình UBND tỉnh xem xét, quyết định ./.

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

Quách Việt Tùng

PHỤ LỤC I

NHỮNG NỘI DUNG CHÍNH CỦA ISO 17799:2005 DÙNG ĐỂ XÂY DỰNG QUY CHẾ NỘI BỘ ĐẢM BẢO AN TOÀN, AN NINH CHO HỆ THỐNG THÔNG TIN.

1. Chính sách an toàn, an ninh thông tin:

Chỉ thị và hướng dẫn về an toàn, an ninh thông tin.

2. An ninh tổ chức:

a) Hạ tầng an ninh thông tin: Quản lý an ninh thông tin trong tổ chức;

b) An ninh đối với bên truy cập thứ ba: Duy trì an ninh cho các phương tiện xử lý thông tin của các tổ chức và tài sản thông tin do các bên thứ ba truy cập.

3. Phân loại và kiểm soát tài sản:

a) Trách nhiệm giải trình tài sản: Duy trì bảo vệ tài sản;

b) Phân loại thông tin tài sản: Đảm bảo mỗi loại tài sản có mức bảo vệ thích hợp.

4. An ninh cá nhân:

a) An ninh trong định nghĩa công việc và nguồn nhân lực: Giảm rủi ro do các hành vi sai sót của con người;

b) Đào tạo người sử dụng: Đảm bảo người sử dụng nhận thức được các mối đe dọa và các vấn đề liên quan đến an ninh thông tin;

c) Đối phó với các sự cố an ninh: Giảm thiểu thiệt hại từ các trục trặc và sự cố an ninh, theo dõi, rút kinh nghiệm.

5. An ninh môi trường và vật lý:

a) Phạm vi an ninh: Ngăn ngừa việc truy cập, gây hại và can thiệp trái phép vào vùng an ninh và thông tin nghiệp vụ;

b) An ninh thiết bị: Để tránh mất mát, lỗi hoặc các sự cố khác liên quan đến tài sản gây ảnh hưởng tới các hoạt động nghiệp vụ;

c) Kiểm soát chung: Ngăn ngừa làm hại hoặc đánh cắp thông tin và các phương tiện xử lý thông tin.

6. Quản lý truyền thông và hoạt động:

a) Thủ tục vận hành và trách nhiệm vận hành hệ thống: Đảm bảo các phương tiện xử lý thông tin hoạt động đúng và an toàn;

b) Lập kế hoạch hệ thống và công nhận: Giảm thiểu rủi ro và lỗi hệ thống;

c) Bảo vệ chống lại phần mềm cố ý gây hại: Bảo vệ tính toàn vẹn của phần mềm thông tin;

d) Công việc quản lý: Duy trì tính toàn vẹn và sẵn sàng của dịch vụ truyền đạt và xử lý thông tin;

đ) Quản trị mạng: Đảm bảo việc an toàn, an ninh thông tin trên mạng và bảo vệ cơ sở hạ tầng kỹ thuật;

g) Trao đổi thông tin: Ngăn ngừa mất mát, thay đổi hoặc sử dụng sai thông tin được trao đổi giữa các đơn vị.

7. Kiểm soát truy cập:

a) Các yêu cầu nghiệp vụ đối với kiểm soát truy cập: Kiểm soát truy cập thông tin;

b) Quản lý truy cập người dùng: Để tránh các truy cập không được cấp phép vào hệ thống;

c) Trách nhiệm của người dùng: để tránh các truy cập của người dùng không được cấp phép;

d) Kiểm soát truy cập mạng: Bảo vệ các dịch vụ mạng;

đ) Kiểm soát truy cập hệ điều hành: Tránh truy cập vào các máy tính không được phép;

g) Kiểm soát truy cập ứng dụng: Tránh truy cập trái phép vào hệ thống;

h) Giám sát truy cập hệ thống và giám sát sử dụng hệ thống: Để phát hiện các hoạt động không được cấp phép;

i) Kiểm soát truy cập từ xa: Đảm bảo an toàn, an ninh thông tin khi sử dụng các phương tiện di động.

8. Phát triển và duy trì hệ thống:

a) Yêu cầu an ninh đối với các hệ thống: Để đảm bảo các yêu cầu an ninh được đưa vào trong quá trình xây dựng hệ thống;

b) An ninh trong hệ thống ứng dụng: Để ngăn ngừa mất mát, thay đổi hoặc lạm dụng cơ sở dữ liệu người sử dụng trong các hệ thống ứng dụng;

c) Các kiểm soát mật mã hóa: Để bảo vệ tính tin cậy, xác thực hoặc toàn vẹn của thông tin;

d) An ninh các File hệ thống: Đảm bảo rằng các dự án công nghệ thông tin và các hoạt động hỗ trợ được quản lý một cách an toàn;

đ) An ninh quá trình hỗ trợ và phát triển: Duy trì an ninh của phần mềm và thông tin hệ thống ứng dụng.

9. Sự tuân thủ:

a) Tuân thủ các yêu cầu pháp lý: Để tránh bất kỳ các vi phạm luật hình sự và dân sự, các nghĩa vụ có tính luật pháp, nguyên tắt và bất kỳ yêu cầu an ninh nào;

b) Soát xét của chính sách an ninh và yêu cầu kỹ thuật để đảm bảo việc tuân thủ của hệ thống với các chính sách và tiêu chuẩn an ninh của Tổ quốc;

c) Xem xét kiểm tra hệ thống: Để tối đa tính hiệu lực để giảm thiểu sự can thiệp tới quy trình kiểm tra hệ thống đó.

PHỤ LỤC II

CÁC BƯỚC CƠ BẢN ĐỂ XÂY DỰNG KHUNG QUY TRÌNH ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Bước 1: Lập kế hoạch bảo vệ an toàn cho hệ thống thông tin

- Thành lập bộ phận quản lý an toàn, an ninh thông tin.

- Xây dựng định hướng cơ bản cho công tác đảm bảo an toàn, an ninh thông tin trong đó chỉ rõ:

+ Mục tiêu ngắn hạn và dài hạn.

+ Phương hướng và văn bản pháp quy, tiêu chuẩn cần tuân thủ và tham khảo.

+ Ước lượng nhân lực và kinh phí đầu tư.

- Lập kế hoạch xây dựng hệ thống bảo vệ an toàn, an ninh thông tin:

+ Xác định và phân loại các nguy cơ gây sự cố an toàn, an ninh thông tin.

+ Rà soát và lập danh sách các đối tượng cần được bảo vệ với những mô tả đầy đủ về: nhiệm vụ; chức năng; mức độ quan trọng và các đặc điểm đối tượng (đối tượng ở đây có thể là phần mềm, máy chủ, quy trình tác nghiệp thuộc cơ quan, đơn vị…)

+ Xây dựng phương án đảm bảo an toàn cho các đối tượng trong danh sách cần được bảo vệ: Nguyên tắc quản lý, vận hành; các giải pháp bảo vệ và khắc phục sự cố…

+ Liên lạc và phối hợp chặt chẽ với Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT), Sở Thông tin và Truyền thông cũng như các cơ quan, tổ chức nghiên cứu và cung cấp dịch vụ an toàn mạng.

+ Lập dự trù kinh phí đầu tư cho hệ thống bảo vệ.

Bước 2. Xây dựng hệ thống bảo vệ an toàn, an ninh thông tin

- Tổ chức đội ngũ nhân viên chuyên trách, đủ năng lực đảm bảo an toàn an ninh thông tin.

- Xây dựng hệ thống bảo vệ an toàn, an ninh thông tin theo kế hoạch

Bước 3. Quản lý và vận hành hệ thống bảo vệ an toàn, an ninh thông tin

- Vận hành và quản lý chặt chẽ trang thiết bị, phần mềm theo đúng quy định đã đặt ra.

- Khi phát hiện sự cố cần nhanh chóng xác định nguyên nhân, tìm biện pháp khắc phục và báo cáo sự cố cho các cơ quan chức năng.

- Cài đặt đầy đủ và thường xuyên cập nhật phần mềm theo hướng dẫn của nhà cung cấp.

Bước 4. Kiểm tra đánh giá hoạt động của hệ thống bảo vệ an toàn, an ninh thông tin

- Thường xuyên kiểm tra giám sát các hoạt động của hệ thống bảo vệ an toàn an ninh thông tin nói riêng cũng như toàn bộ hệ thống thông tin nói chung.

- Báo cáo tổng kết tình hình theo định kỳ.

Bước 5. Bảo trì và nâng cấp hệ thống bảo vệ an toàn, an ninh thông tin

Thường xuyên kiểm tra và bảo trì hệ thống bảo vệ an toàn, an ninh thông tin. Cần nhanh chóng mở rộng, nâng cấp hoặc thay đổi khi cần thiết./.