ỦY BAN NHÂN DÂN TỈNH ĐỒNG NAI	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số:34/2009/QĐ-UBND	*Biên Hòa, ngày 21 tháng 5 năm 2009*

QUYẾT ĐỊNH

Ban hành Quy chế đảm bảo an toàn, an ninh thông tin trong lĩnh vực ứng dụng công nghệ thông tin của các cơ quan, đơn vị quản lý hành chính nhà nước trên địa bàn tỉnh Đồng Nai

ỦY BAN NHÂN DÂN TỈNH ĐỒNG NAI

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

Căn cứ Luật Giao dịch điện tử ngày 29 tháng 11 năm 2005;

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

Căn cứ Chỉ thị số 03/2007/CT-BBCVT ngày 23 tháng 2 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 tại Tờ trình số 224/TTr- STTT ngày 07/04/2009,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo quyết định này Quy chế đảm bảo an toàn, an ninh thông tin trong lĩnh vực ứng dụng công nghệ thông tin của các cơ quan, đơn vị quản lý hành chính nhà nước trên địa bàn tỉnh Đồng Nai.

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

Điều 3. Chánh Văn phòng Ủy ban nhân dân tỉnh, Giám đốc các Sở, ban, ngành, Chủ tịch Ủy ban nhân dân các huyện, thị xã Long Khánh, thành phố Biên Hòa có trách nhiệm thi hành quyết định này./.

Nơi nhận:
- Cục kiểm tra văn bản QPPL (Bộ Tư Pháp);
- Bộ Thông tin và Truyền thông;
- Như điều 3 (để thực hiện);
- Thường trực Tỉnh ủy (để báo cáo);
- Thường trực HĐND tỉnh;
- Chủ tịch, các Phó Chủ tịch UBND tỉnh;
- Lưu VT –TH (các phòng, TT).

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Võ Văn Một

ỦY BAN NHÂN DÂN TỈNH ĐỒNG NAI	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 lĩnh vực ứng dụng công nghệ thông tin của các cơ quan, đơn vị quản lý hành chính nhà nước trên địa bàn tỉnh Đồng Nai

(Ban hành kèm theo Quyết định số 34/2009/QĐ-UBND ngày 21 tháng 5 năm 2009 của Ủy ban nhân dân tỉnh Đồng Nai)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về công tác đảm bảo an toàn an ninh thông tin trong lĩnh vực ứng dụng công nghệ thông tin phục vụ cho công tác điều hành và quản lý hành chính nhà nước trên địa bàn.

Điều 2. Đối tượng áp dụng

Quy chế này được áp dụng đối với tất cả cơ quan, đơn vị quản lý hành chính nhà nước trên địa bàn tỉnh Đồng Nai.

Điều 3.Giải thích từ ngữ

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

1. An toàn thông tin (ATTT): bao gồm các hoạt động quản lý, nghiệp vụ và kỹ thuật đối với hệ thống thông tin nhằm bảo vệ, khôi phục các hệ thống, các dịch vụ và nội dung thông tin đối với nguy cơ tự nhiên hoặc do con người gây ra. Việc bảo vệ thông tin, tài sản và con người trong hệ thống thông tin nhằm bảo đảm cho các hệ thống thực hiện đúng chức năng, phục vụ đúng đối tượng một cách sẵn sàng, chính xác và tin cậy. An toàn thông tin bao hàm các nội dung bảo vệ và bảo mật thông tin, an toàn dữ liệu, an toàn máy tính và an toàn mạng.

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

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

4. Tính sẵn sàng: đảm bảo những người được cấp quyền có thể truy nhập thông tin và các tài sản liên quan ngay khi có nhu cầu.

5. TCVN 7562: 2005: tiêu chuẩn Việt Nam về mã thực hành quản lý ATTT.

6. 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).

7. 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 4. Các biện pháp quản lý vận hành trong công tác an toàn an ninh thông tin

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

2. Các cơ quan, đơn vị cần xác định cán bộ chuyên trách về an toàn hệ thống thông tin. Cán bộ này cần phải có các kiến thức về an toàn, an ninh thông tin trước khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ.

3. Cán bộ chuyên trách tại các cơ quan, đơn vị được thủ trưởng đơn vị đảm bảo điều kiện học tập, tiếp thu công nghệ, kiến thức an toàn bảo mật thông tin.

4. Cán bộ chuyên trách an toàn hệ thống thông tin chịu trách nhiệm tham mưu chuyên môn và vận hành an toàn hệ thống thông tin của đơn vị theo nhiệm vụ được thủ trưởng đơn vị phân công.

5. Cán bộ chuyên trách cần cập nhật cấu hình chuẩn cho các thành phần của hệ thống khi tiến hành cài đặt và thiết lập cấu hình chặt chẽ nhất cho các sản phẩm an toàn thông tin nhưng vẫn duy trì yêu cầu hoạt động của hệ thống thông tin.

6. Cán bộ chuyên trách cần 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 dịch vụ không cần thiết.

7. Cán bộ chuyên trách cần 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.

8. Cán bộ chuyên trách cần 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 tháo lắp 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 (sử dụng một hãng cho máy chủ và hãng khác cho máy trạm).

9. Cán bộ chuyên trách cần 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.

10. Các cơ quan, đơn vị cần hủy 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 (khóa, thẻ nhận

dạng,...) đối với nhân viên đã chấm dứt hợp đồng và đảm bảo khả năng vẫn truy nhập được vào các hồ sơ được tạo ra bởi nhân viên đó.

11. Các cơ quan, đơn vị xác định và phân bổ đầu tư cần thiết để bảo vệ hệ thống thông tin.

Điều 5. Các biện pháp quản lý kỹ thuật cho công tác an toàn an ninh thông tin

1. 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 1 lần/1 năm và triển khai các công cụ tự động để hỗ trợ việc quản lý các tài khoản của hệ thống thông tin.

2. Hệ thống thông tin giới hạn một số hữu hạn lần đăng nhập sai liên tiếp. 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.

3. Tổ chức theo dõi, và kiểm soát tất cả các phương pháp truy nhập từ xa (quay số, Internet...) 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.

4. 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.

5. Hệ thống thông tin cần ghi nhận 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.

6. Tổ chức quản lý định danh người dùng.

7. Hệ thống thông tin cần ngăn chặn hoặc hạn chế các sự cố gây ra do tấn công từ chối dịch vụ. Cán bộ chuyên trách có thể sử dụng các thiết bị đặt tại biên của mạng lọc gói tin để bảo vệ các thiết bị bên trong, tránh bị ảnh hưởng trực tiếp bởi tấn công từ chối dịch vụ. Đối với hệ thống thông tin cho phép truy nhập công cộng thì có thể được bảo vệ bằng cách tăng dung lượng, băng thông hoặc thiết lập hệ thống dự phòng.

Điều 6. Xây dựng quy chế nội bộ đảm bảo an toàn cho hệ thống thông tin.

1. Các cơ quan đơn vị quản lý hành chính nhà nước 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.

e) 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 4 và điều 5 của Quy chế.

f) 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.

h) Tổ chức thực hiện.

2. Các cơ quan, đơn vị xây dựng quy chế an toàn an ninh cho đơn vị căn cứ các tiêu chuẩn kỹ thuật quản lý an toàn của bộ tiêu chuẩn TCVN 7562:2005 và ISO/IEC 17799:2005 tại phụ lục I để có sự lựa chọn áp dụng phù hợp từng cơ quan, đơn vị mình.

Điều 7. Xây dựng và áp dụng quy trình đảm bảo an toàn, an ninh cho hệ thống thông tin

1. Các cơ quan, đơn vị quản lý hành chính 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;

e) 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 và tiêu chuẩn quốc tế ISO 27001.

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

Điều 8. Trách nhiệm của các cơ quan, đơn vị quản lý hành chính Nhà nước

1. Thủ trưởng các cơ quan, đơn vị có trách nhiệm thực hiện Điều 6 và Điều 7 của Quy chế này và chịu trách nhiệm toàn diện trước UBND tỉnh trong công tác bảo vệ an toàn hệ thống thông tin của đơn vị.

2. Khi có sự cố hoặc nguy cơ mất an toàn 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 ATTT của 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 theo biểu mẫu tại phụ lục III. Trường hợp có sự cố nghiêm trọng vượt quá khả năng khắc phục của đơn vị, phải báo cáo ngay cho cơ quan cấp trên quản lý trực tiếp và Sở Thông tin và Truyền thông.

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 xuất trình.

5. Báo cáo tình hình an toàn, an ninh thông tin theo biểu mẫu tại phụ lục IV gửi về Sở Thông tin và Truyền thông định kỳ hằng năm 1 lần vào cuối quý III.

Điều 9. Trách nhiệm của cán bộ công chức trong các cơ quan, đơn vị quản lý hành chính nhà nước

1. Nghiêm chỉnh thi hành các quy chế nội bộ, quy trình về ATTT 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 ninh thông tin tại 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 đề ra.

Điều 10. 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 và chịu trách nhiệm trước UBND tỉnh trong việc đảm bảo an toàn an ninh cho các hệ thống thông tin cấp tỉnh.

2. Thành lập Đoàn kiểm tra an toàn, an ninh thông tin và tiến hành kiểm tra, xử phạt theo định kỳ hoặc kiểm tra đột xuất khi phát hiện có các dấu hiệu, hành vi vi phạm an toàn, an ninh thông tin.

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

4. Tuỳ 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.

5. Hướng dẫn, giám sát các đơn vị xây dựng quy chế đảm bảo an toàn, an ninh cho hệ thống thông tin theo qui định của Nhà nước.

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

Điều 11. Kế hoạch kiểm tra hàng năm

1. Sở Thông tin và Truyền thông chủ trì, phối hợp Văn phòng UBND tỉnh, Công an tỉnh và các đơn vị có liên quan tiến hành công tác kiểm tra an toàn, an ninh thông tin tại tất cả các đơn vị hành chính cấp tỉnh, huyện định kỳ hàng năm tối thiểu 1 lần vào quý III, kiểm tra tại cơ sở cấp phường/xã theo kế hoạch của Sở Thông tin và Truyền thông.

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

Điều 12. 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 chính trong việc chủ trì và 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) Tiến hành xử phạt 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 nhà nước trên địa bàn tỉnh;

c) Tuyên truyền công tác an tòan, an ninh thông tin tại các đơn vị hành chính trên địa bàn tỉnh.

2. Văn phòng UBND tỉnh:

a) Cử bộ phận chuyên trách an toàn an ninh thông tin phối hợp Sở Thông tin và Truyền thông kiểm tra, đánh giá công tác an toàn an ninh thông tin.

b) Phối hợp xây dựng các tiêu chí và quy trình kỹ thuật kiểm tra công tác an toàn, an ninh thông tin.

3. 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 lí các trường hợp vi phạm an toàn, an ninh thông tin theo thẩm quyền.

Chương V
KHEN THƯỞNG, XỬ LÝ VI PHẠM

Điều 13. Khen thưởng

Hằng năm, Sở Thông tin và Truyền thông dựa trên các điều tra, báo cáo công tác ATTT của các cơ quan, đơn vị để xác lập bảng xếp hạng ATTT; trên cơ sở đó đề xuất UBND tỉnh xét khen thưởng các cá nhân, đơn vị theo quy định hiện hành.

Điều 14. Xử lý vi phạm

Tổ chức, cá nhân có hành vi vi phạm quy chế này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật theo trách nhiệm, xử phạt hành chính hoặc bị truy

cứu trách nhiệm hình sự. Nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật hiện hành.

Chương VI
ĐIỀU KHOẢN THI HÀNH

Điều 15. Sở Thông tin và Truyền thông chủ trì, phối hợp với các sở, ban ngành, UBND các huyện, thị xã Long Khánh, thành phố Biên Hòa và các cơ quan có liên quan triển khai thực hiện Quy chế này.

Điều 16. 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
CHỦ TỊCH

Võ Văn Một

Phụ lục I

10 NỘI DUNG CHÍNH CỦA ISO/IEC 17799:2005 DÙNG ĐỂ XÂY DỰNG QUY CHẾ NỘI BỘ ĐẢM BẢO AN TOÀN CHO HỆ THỐNG THÔNG TIN

(Ban hành kèm theo Quyết định số: /2009/QĐ-UBND ngày tháng năm 2009 của Ủy ban nhân dân tỉnh Đồng Nai)

1. Chính sách an toàn thông tin: chỉ thị và hướng dẫn về an toàn 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 tổ chức và tài sản thông tin do các bên thứ ba truy nhập.

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 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 sực cố an ninh: giảm thiểu thiệt hại từ các trục trặc và sự cố an ninh, theo dõi và 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 về lỗi hệ thống.

c) Bảo vệ chống lại phần mềm cố ý gây hại: bảo vệ tính toàn vẹn của phần mềm và 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.

e) Quản trị mạng: đảm bảo việc an toàn thông tin trên mạng và bảo vệ cơ sở hạ tầng kỹ thuật.

f) Trao đổi thông tin: ngăn ngừa mất mát, thay đổi hoặc sử dụng sai thông tin được trao đổi giữa các đơn vi.

7. Kiểm soát truy cập:

a) Các yêu cầu nghiệp vụ đối với kiểm soát truy nhập: kiểm soát truy nhập thông tin.

b) Quản lý truy nhập của người dùng: để tránh các truy nhập không được cấp phép vào hệ thống.

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

d) Kiểm soát truy nhập mạng: bảo vệ các dịch vụ mạng.

e) Kiểm soát truy nhập hệ điều hành: tránh truy nhập vào các máy tính không được phép.

f) Kiểm soát truy nhập ứng dụng: tránh các truy nhập trái phép vào hệ thống.

g) Giám sát truy nhập hệ thống và giám sát sử dụng hệ thống: để phát hiện các hoạt động không được cấp phép.

h) Kiểm soát truy cập từ xa: đảm bảo 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 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 tệp 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.

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

9. Quản lý liên tục trong kinh doanh: chống lại sự gián đoạn trong các hoạt động kinh doanh.

10. Sự tuân thủ:

a) Tuân thủ các yêu cầu pháp lý: để tránh các vi phạm bất kỳ luật hình sự và dân sự, các nghĩa vụ có tính luật pháp, nguyên tắc 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 CHO HỆ THỐNG THÔNG TIN

(Ban hành kèm theo Quyết định số: 34/2009/QĐ-UBND ngày 21 tháng 5 năm 2009 của Ủy ban Nhân dân tỉnh Đồng Nai)

Bước 1: Lập kế hoạch bảo vệ an toàn an ninh 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 một phần mềm, máy chủ, quy trình tác nghiệp thuộc cơ quan đơn vị v.v...).
  - 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 v.v...
  - Liên lạc và hợp tác 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 kế hoạch 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 cho hệ thống 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.

Phụ lục III

MẪU BÁO CÁO SỰ CỐ

(Ban hành kèm theo Quyết định số 34/2009/QĐ-UBND ngày 21 tháng 5 năm 2009 của Ủy ban Nhân dân tỉnh Đồng Nai)

Đơn vị: .....
.....
.....

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

Ngày tháng năm

- Họ và tên *.....
- Cơ quan *.....
- Email * .....
- Điện thoại * .....

Thông tin về sự cố

- Mô tả sơ bộ về sự cố *.....
  .....
  .....
- Cách thức phát hiện * (*Đánh dấu những cách thức được sử dụng để phát hiện sự cố*)
  ☐ Qua hệ thống IDS ☐ Kiểm tra Log File ☐ Quản trị hệ thống
  ☐ Khác, đó là .....
- Thời gian xảy ra sự cố *: .../... /...../.../... (ngày/tháng/năm/giờ/phút)
  (Ngày,Tháng điền đủ 2 chữ số,Năm điền đủ 4 chữ số,Giờ,Phút điền đủ 2 chữ số theo hệ 24 giờ)
- Thời gian thực hiện báo cáo sự cố *: .../... /.../...(ngày/tháng/năm/giờ/phút)

Thông tin về hệ thống xảy ra sự cố

- Hệ điều hành *.....Version * .....
- Các dịch vụ có trên hệ thống (*Đánh dấu những dịch vụ được sử dụng trên hệ thống*)
  ☐ Web server ☐ Mail server ☐ Database server
  ☐ FTP server ☐ Proxy server ☐ Application server
  ☐ Dịch vụ khác, đó là .....

- Các địa chỉ IP của hệ thống (*)

(Chỉ liệt kê các địa chỉ IP được sử dụng trên Internet, không cần liệt kê các địa chỉ IP nội bộ)

.....

.....

- Các tên miền của hệ thống (*)

.....

.....

- Mục đích chính sử dụng hệ thống * .....

.....

.....

Người báo cáo sự cố

Phụ lục IV

MẪU BÁO CÁO TÌNH HÌNH AN TOÀN, AN NINH THÔNG TIN

(Ban hành kèm theo Quyết định số:34/2009/QĐ-UBND ngày 21 tháng 5 năm 2009 của Ủy ban Nhân dân tỉnh Đồng Nai)

Đơn vị: .....
.....
.....

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

Ngày tháng năm

Báo cáo Tình hình an toàn, an ninh thông tin

Chú ý:

- Điền thông tin đầy đủ vào các câu hỏi

- Để lựa chọn đánh dấu X

- Câu hỏi với ký hiệu O trước mỗi lựa chọn thì chỉ được phép đánh dấu một kết quả (chọn một)

- Câu hỏi với ký hiệu □ trước mỗi lựa chọn thì có thể đánh dấu từ không tới nhiều kết quả (chọn nhiều)

- Ký, ghi tên và đóng dấu đầy đủ vào cuối báo cáo và gửi về theo đường công văn cho Sở Thông tin và Truyền thông.

I. Đánh giá hiện trạng và dự kiến

1. Về chính sách, quản lý

Đơn vị:

❖ **Đã xây dựng chiến lược để đảm bảo an toàn thông tin cho tổ chức mình chưa?**

O Rồi O Chưa

❖ **Có các biện pháp vận hành liên tục và khôi phục sau sự cố không?**

O Có O Không

❖ **Có thường xuyên cập nhật công nghệ đảm bảo an toàn thông tin hay không?**

O Có O Không

❖ **Nếu tự đánh giá, mức độ đảm bảo an toàn thông tin của đơn vị trong năm 20.. là:**

Kém		Trung bình	Tốt		Rất tốt
O 0	O 1	O 2	O 3	O 4	O 5

2. Về đầu tư

Đơn vị:

❖ **Phần trăm ngân sách trong tổng số ngân sách cho công nghệ thông tin để đầu tư vào việc đảm bảo an toàn thông tin: .....%**

❖ **Đã và dự kiến đầu tư vào vấn đề nào dưới đây**

Lĩnh vực	20..	Dự kiến 20..	Dự kiến 20..-20..
Xây dựng chính sách/hướng dẫn/thủ tục	☐	☐	☐
Sử dụng dịch vụ	☐	☐	☐
Yêu cầu tư vấn	☐	☐	☐
Mua thiết bị an toàn thông tin	☐	☐	☐
Mua phần mềm an toàn thông tin	☐	☐	☐
Nghiên cứu sử dụng phần mềm mã nguồn mở	☐	☐	☐
Đào tạo nhân lực	☐	☐	☐
Vấn đề khác, đó là:			

❖ **Đã và dự kiến sử dụng những công cụ đảm bảo an toàn thông tin nào**

Công cụ	20..	Dự kiến 20...	Dự kiến 20..-20..
Công cụ diệt virus (Antivirus)	☐	☐	☐

Công cụ diệt Adware/Spyware	☐	☐	☐
Mật khẩu	☐	☐	☐
Tường lửa (Firewall)	☐	☐	☐
Công cụ lọc thư rác	☐	☐	☐
Công cụ mã hóa tệp tin	☐	☐	☐
Công cụ chống DdoS	☐	☐	☐
Hạ tầng khóa công khai (PKI)	☐	☐	☐
Mạng riêng ảo (VPN)	☐	☐	☐
Hệ thống phát hiện xâm nhập (IDS)	☐	☐	☐
Những công nghệ khác, đó là			

3. Về tình hình an ninh mạng và xử lý sự cố

❖ **Tổng kết về các sự cố an ninh mạng đã xảy ra trong năm 20.. đối với đơn vị**

Sự cố	Số lượng
Virus	
Lừa phỉnh (phishing)	
Thư rác (Spam mail)	
Spyware/Adware	
Tấn công từ chối dịch vụ (DoS, DDoS)	
Nội dung website đơn vị bị thay đổi (deface website)	
Sự cố khác: - .... - .... -	

❖ **Mức độ thiệt hại ước tính trong năm 20.. do các sự cố an ninh mạng gây ra**

☐ Thiệt hại gián tiếp:..... triệu đồng

☐ Thiệt hại trực tiếp:..... triệu đồng

☐ Chi phí khắc phục:..... triệu đồng

❖ **Biện pháp xử lý đã áp dụng khi gặp sự cố**

Phương pháp	Số lần
Không làm gì cả	
Tự xử lý	
Báo cáo cấp trên trực tiếp	
Yêu cầu hỗ trợ từ nơi khác	
Báo cảnh sát mạng	
Biện pháp khác, đó là: - .... - .... -	

❖ **Cho biết công việc mà cơ quan đã thực hiện sau khi khắc phục được sự cố trong năm qua:**

☐ Sửa đổi chính sách/hướng dẫn/thủ tục

☐ Nâng cao ý thức

☐ Tăng cường thiết bị

☐ Rà soát lại hệ thống

☐ Mở rộng liên kết với các đơn vị hoạt động trong lĩnh vực an toàn thông tin

☐ Việc khác, đó là :

.....

4. Tổ chức nhân lực và bồi dưỡng nghiệp vụ

❖ **Đơn vị có bộ phận phụ trách về đảm bảo an toàn, an ninh thông tin không?**

O Có O Không

- Nếu có, bộ phận đó có người phụ trách là:

O Lãnh đạo cơ quan O Giám đốc CNTT O Nhân viên chuyên trách O Khác: ..... **- Nếu chưa, thì đơn vị có dự kiến tổ chức bộ phận đó không?**

O Có O Không

Dự kiến sẽ thành lập vào tháng.....năm....., với số cán bộ là ..... người

❖ **Đơn vị có nhu cầu bồi dưỡng nghiệp vụ an toàn thông tin:**

☐ Dành cho lãnh đạo và cán bộ quản lý. Số lượng dự kiến: ... người

☐ Cơ bản/nâng cao về an toàn thông tin cho cán bộ kỹ thuật Số lượng dự kiến: ... người

☐ Kỹ năng an toàn thông tin cho người dùng máy tính. Số lượng dự kiến: ... người

❖ **Đơn vị đã có dự trù kinh phí cho huấn luyện nghiệp vụ, đào tạo phát triển nguồn nhân lực đảm bảo an ninh thông tin của đơn vị hay chưa?**

O Có O Chưa

II. Ý kiến phản hồi và góp ý thêm

.....
.....
.....
.....

Thủ trưởng đơn vị
(Ký tên và đóng dấu)