

Số: 4139 /QĐ-UBND

Tây Sơn, ngày 24 tháng 12 năm 2012

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 quản lý hành chính nhà nước huyện Tây Sơn

ỦY BAN NHÂN DÂN HUYỆN

Căn cứ Luật Tổ chức HĐND và UBND 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 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 Chỉ thị số 897/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 22/2012/QĐ-UBND ngày 12 tháng 7 năm 2012 của UBND tỉnh Bình Định về việc ban hành 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 quản lý hành chính nhà nước tỉnh Bình Định;

Xét đề nghị của Chánh Văn phòng HĐND và UBND huyện,

QUYẾT ĐỊNH:

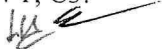
Điều 1. Ban hành kèm theo Quyết định này Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan quản lý hành chính nhà nước huyện Tây Sơn.

Điều 2. Giao Chánh Văn phòng HĐND và UBND huyện phối hợp cùng Phòng Văn hóa và Thông tin huyện tổ chức triển khai thực hiện Quyết định này.

Điều 3: Chánh Văn phòng HĐND và UBND huyện, Trưởng phòng Văn hóa và Thông tin huyện, các phòng, ban, ngành; Chủ tịch UBND các xã, thị trấn và Thủ trưởng các cơ quan, đơn vị, tổ chức, cá nhân liên quan chịu trách nhiệm thi hành Quyết định này kể từ ngày ký./.

Nơi nhận:

- Như Điều 3;
- TT.Huyện Ủy,
- TT.HĐND huyện;
- CT, các PCT UBND huyện;
- C,PVP; CV;
- Lưu: VT, C3.



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



Đỗ Văn Lợi

QUY CHẾ

**Đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng
Công nghệ thông tin của các cơ quan quản lý nhà nước huyện Tây Sơn**
(Ban hành kèm theo Quyết định số 4139 /QĐ-UBND ngày 24/12/2012
của UBND huyện Tây Sơn)

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 hoạt động ứng dụng công nghệ thông tin (CNTT) của các cơ quan quản lý nhà nước thuộc huyện Tây Sơn.

Điều 2. Đối tượng áp dụng

Quy chế này được áp dụng đối với các cơ quan quản lý nhà nước thuộc huyện, bao gồm: các phòng, ban, ngành, UBND các xã, thị trấn, các đơn vị sự nghiệp thuộc huyện (sau đây gọi tắt là các cơ quan, đơn vị).

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

1. Giảm thiểu được các nguy cơ gây mất sự cố an toàn thông tin và đảm bảo an ninh thông tin trong quá trình tác nghiệp của cán bộ, công chức, viên chức.
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 hoạt động của các cơ quan quản lý hành chính nhà nước.

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.
3. *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.
4. *TCVN 7562:2005*: Tiêu chuẩn Việt Nam về mã thực hành quản lý an toàn thông tin.
5. *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).

6. *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.

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

8. *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 cá nguy cơ tự nhiên, các hành động truy cập, sử dụng, phát tán, phá hoại, sử dụng và phá hủy bất hợp pháp, mục đích 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. 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.

9. *Virus máy tính*: Là 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. *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.

11. *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.

12. *Giao thức*: Là tập hợp các quy tắc, quy ước truyền thông của mạng mà tất cả các thực thể tham gia truyền thông phải tuân theo.

13. *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. Bản ghi nhật ký hệ thống dùng để phân tích những sự kiện đã xảy ra, nguồn gốc và các kết quả để có các biện pháp xử lý thích hợp.

14. *Mạng ngang hàng*: là mạng mà trong đó các máy tính có quyền bình đẳng như nhau, mỗi máy tính có quyền chia sẻ tài nguyên và sử dụng các tài nguyên từ máy tính khác.

Chương II

QUY ĐỊNH ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

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

1. Đối với các cơ quan, đơn vị:

a) Trang bị đầy đủ các 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 chuyên trách về an toàn hệ thống thông tin (sau đây gọi tắt là cán bộ chuyên trách). Cán bộ chuyên trách được đảm bảo điều kiện học tập, tiếp cận công nghệ, kiến thức an toàn bảo mật thông tin trước khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ.

c) Xác định và phân bổ kinh phí chi thường xuyên 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 các máy trạm, máy chủ,... và các công việc khác có liên quan đến việc bảo đảm an toàn, an ninh thông tin.

d) Phải bố trí ít nhất 01 máy vi tính riêng, không kết nối mạng nội bộ và Internet dùng để soạn thảo văn bản, lưu giữ thông tin có nội dung mật theo quy định.

e) Kiểm tra việc thực hiện các nội dung của Điều 6 Quy chế này.

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

a) Triển khai, thực hiện các nội dung của Điều 6 Quy chế này.

b) Tham mưu cho lãnh đạo triển khai thực hiện các biện pháp để đảm bảo an toàn, an ninh hệ thống thông tin của cơ quan, đơn vị. Thường xuyên nghiên cứu, cập nhật các kiến thức về an toàn, an ninh thông tin, có biện pháp phòng tránh các nguy cơ tiềm ẩn có thể gây mất thông tin khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ.

c) Thường xuyên cập nhật cấu hình chuẩn cho các thành phần của hệ thống thông tin, thiết lập cấu hình chặt chẽ nhất nhưng vẫn đảm bảo duy trì hoạt động thường xuyên của hệ thống thông tin.

d) Khi tổ chức cấu hình hệ thống thông tin chỉ cung cấp những chức năng thiết yếu nhất; xác định các chức năng, cổng giao tiếp mạng, giao thức, và dịch vụ không cần thiết để cấm hoặc hạn chế sử dụng.

e) Thường xuyên thực hiện việc theo dõi bản ghi nhật ký hệ thống và các sự kiện khác có liên quan để 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.

f) Kiểm soát chặt chẽ cài đặt phần mềm vào máy trạm và máy chủ.

3. Đối với cán bộ, công chức, viên chức:

a) Thường xuyên cập nhật những chính sách, thủ tục an toàn thông tin của cơ quan, đơn vị và thực hiện đúng hướng dẫn về an toàn, an ninh thông tin của cán bộ chuyên trách.

b) Hạn chế việc sử dụng chức năng chia sẻ tài nguyên (sharring), khi sử dụng chức năng này cần bật thuộc tính bảo mật bằng mật khẩu và thu hồi chức năng này khi đã sử dụng xong.

c) Các máy tính khi không sử dụng trong thời gian dài (quá 4 giờ làm việc) cần tắt máy hoặc ngưng kết nối mạng, để tránh bị các tin tặc lợi dụng, sử dụng chức năng điều khiển từ xa dùng máy tính của mình tấn công vào các hệ thống thông tin khác.

d) Khi mở các tập tin đính kèm theo thư điện tử, nếu biết rõ gửi thư thì phải lưu tập tin vào máy tính thực hiện quét virus trước khi mở các tập tin đính kèm theo thư điện tử, không mở các thư điện tử khi chưa rõ người gửi hoặc tập tin đính kèm có nguồn gốc không rõ ràng để tránh virus, phần mềm gián điệp lây nhiễm máy tính.

e) Phải đặt mật khẩu cho máy tính (mật khẩu đăng nhập, mật khẩu bảo vệ màn hình). Sử dụng các thiết bị lưu trữ thông tin (USB, ổ cứng gắn ngoài, thẻ nhớ...) đảm bảo an toàn, đúng cách để phòng ngừa virus, phần mềm gián điệp xâm nhập máy tính phá hoại, đánh cắp thông tin.

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

1. Tổ chức mô hình mạng:

Cài đặt, cấu hình, tổ chức hệ thống mạng theo mô hình Clients/Server, hạn chế sử dụng mô hình mạng ngang hàng. Các cơ quan, đơn vị có nhiều phòng, ban, đơn vị trực thuộc không nằm trong cùng một khu vực, cần thiết lập mạng riêng ảo (Virtual Private Network - VPN) để đảm bảo an ninh cho mạng nội bộ. Khi thiết lập các dịch vụ trên môi trường mạng Internet, chỉ cung cấp những chức năng thiết yếu nhất bảo đảm duy trì hoạt động của hệ thống thông tin; hạn chế sử dụng chức năng, cổng giao tiếp mạng, giao thức và các dịch vụ không cần thiết.

2. Quản lý hệ thống mạng không dây: Khi thiết lập mạng không dây để kết nối với mạng cục bộ thông qua các điểm truy nhập (Access Point - AP), cần thiết lập các tham số như: tên, SSID (Service Set Identification – Dịch vụ thiết lập nhận dạng), mật khẩu, mã hóa dữ liệu và thông báo các thông tin liên quan đến điểm truy nhập để cơ quan sử dụng, thường xuyên thay đổi mật khẩu nhằm tăng cường công tác bảo mật.

3. Tổ chức quản lý tài khoản của các hệ thống thông tin, bao gồm: Tạo mới, kích hoạt, sử 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 06 tháng/ lần và triển khai các công tự hủy tự động để hỗ trợ việc quản lý tài khoản của hệ thống thông tin. Hủy tài khoản, quyền truy cập hệ thống thông tin, thu hồi lại tất cả các tài sản liên quan để hệ thống thông tin (khóa, thẻ nhận dạng, thư mục lưu trữ,...) đối với cán bộ, nhân viên đã chuyển công tác, chấm dứt hợp đồng.

4. Quản lý đăng nhập hệ thống: Các hệ thống thông tin cần giới hạn một số hữu hạn lần đăng nhập sai liên tiếp. Nếu liên tục đăng nhập sai vượt quá số lần quy định thì hệ thống phải tự động khóa tài khoản hoặc cô lập tài khoản trong một khoảng thời gian nhất định trước khi tiếp tục cho đăng nhập. 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 quản trị, tăng cường sử dụng mạng riêng ảo (VPN - Virtual Private Network) khi có nhu cầu làm việc từ xa; yêu cầu người dùng đặt mật khẩu với độ an toàn cao (có chữ thường, có chữ in hoa, có số và ký tự đặc biệt như @, #, !...) và thường xuyên thay đổi mật khẩu. Hệ thống thông tin cần có cơ chế kiểm tra, cho phép ứng với mỗi phương pháp truy nhập từ xa và cơ chế tự động giám sát điều khiển các truy cập từ xa.

5. Quản lý Logfile: Hệ thống thông tin cần ghi nhận các sự kiện cần thiết phục vụ quá trình kiểm soát: quá trình đăng nhập hệ thống, các thao tác cấu hình hệ thống, quá trình truy xuất hệ thống; ghi nhận đầy đủ thông tin 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 trữ nhật ký trong một khoảng thời gian nhất định.

6. Chống mã độc, virus: Lựa chọn, triển khai các phần mềm chống virus, thư rác có hiệu quả trên các máy chủ, máy trạm, các thiết bị, phương tiện kỹ thuật trong mạng, các hệ thống thông tin quan trọng như: Cổng/Trang thông tin điện tử, thư điện tử, một cửa điện tử,...; đồng thời, thường xuyên cập nhật phiên bản mới, bản vá lỗi của các phần mềm chống virus, nhằm kịp thời phát hiện, loại trừ mã độc máy tính (Virus, trojan, worms,...) và hỗ trợ người sử dụng cài các phần mềm này trên máy trạm. Thường xuyên cập nhật các phiên bản mới, các bản vá lỗi các phần mềm chống virus để bảo đảm chương trình quét virus cấu cơ quan trên các máy chủ, máy trạm luôn được cập nhật mới nhất, phù hợp với quy trình và chính sách quản lý hệ thống thông tin của tổ chức, thiết lập chế độ quét thường xuyên ít nhất là hàng tuần.

7. Tổ chức quản lý tài nguyên: Kiểm tra, giám sát chức năng chia sẻ thông tin (Network File and Folder Sharing). Tổ chức cấp phát tài nguyên trên máy chủ theo danh mục thư mục cho từng phòng/ban; khuyến cáo người sử dụng cân nhắc việc chia sẻ tài nguyên cục bộ trên máy đang sử dụng, khi thực hiện việc chia sẻ tài nguyên cần phải sử dụng mật khẩu để bảo vệ thông tin.

8. Thiết lập cơ chế sao lưu và phục hồi máy chủ, máy trạm:

a) Đối với máy trạm, máy chủ: thực hiện việc sao lưu dữ liệu như hệ điều hành, các phần mềm ứng dụng, phần mềm chuyên ngành, cơ sở dữ liệu chuyên môn, quan trọng phục vụ công tác của cơ quan, đơn vị bằng các phần mềm chuyên dụng. Thời gian định kỳ tiến hành sao lưu dữ liệu tùy thuộc từng cơ quan, đơn vị. Thời gian định kỳ tiến hành sao lưu vào các thiết bị lưu trữ như CD, ổ cứng ngoài,... và thực hiện việc đánh số, dán nhãn để tránh nhầm lẫn, cá thiết bị lưu trữ này được cất giữ nơi an toàn, bảo mật nhằm phục vụ công tác phục hồi dữ liệu một cách nhanh nhất.

b) Đối với máy chủ: Bảo đảm thiết lập cơ chế sao lưu phục hồi hệ thống máy chủ. Đối với các máy chủ cài đặt hệ điều hành Windows sử dụng chức năng System Restore để có thể dễ dàng khôi phục lại toàn bộ máy chủ hoặc các tập tin, thư mục được lựa chọn phục hồi.

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

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

Bước 2: Sao chép logfile và toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ (phục vụ cho công tác phân tích).

Bước 3: Khôi phục hệ thống bằng cách chuyển dữ liệu backup mới nhất để hệ thống hoạt động.

Bước 4: Thực hiện cá công việc được quy định tại khoản 2 Điều 9.

10. Hệ thống thông tin tại các cơ quan, đơn vị cần có cơ chế ngăn chặn hoặc hạn chế các sự cố gây ra do tấn công từ chối dịch vụ (DoS, DDoS). Sử dụng các thiết bị để lọc các gói tin nhằm 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 có thể thực hiện bảo vệ bằng cách tăng dung lượng, băng thông hoặc thiết lập hệ thống dự phòng.

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.

e) Kiểm tra, khắc phục sự cố an toàn, an ninh của hệ thống thông tin bằng cách sử dụng các biện pháp trong Điều 4 và Điều 5 của Quy chế này.

f) Nguyên tắc chung về sử dụng an toàn và hiệu quả đối với các 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) Các biện pháp tổ chức thực hiện.

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 của bộ tiêu chuẩn TCVN 7562:2005 và ISO/IEC 17799:2005 tại Phụ lục 1 kèm theo Quy chế này, để áp dụng cho 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 ra 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 2 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 8. Trách nhiệm của các cơ quan, đơn vị

1. Thủ trưởng các cơ quan, đơn vị có trách nhiệm tuyên truyền, nâng cao nhận thức cho cán bộ, công chức, viên chức về các nguy cơ mất an toàn, an ninh hệ thống thông tin; tổ chức triển khai thực hiện các quy định tại Quy chế này và chịu trách nhiệm trước UBND huyện trong công tác đảm bảo an toàn, an ninh thông tin của cơ quan, đơn vị mình.

2. Khi có sự cố hoặc nguy cơ mất an toàn thông tin phải kịp thời chỉ đạo khắc phục ngay, ưu tiên sử dụng cán bộ kỹ thuật chuyên trách trong cơ quan, đơn vị và thông báo bằng văn bản cho UBND huyện (qua Văn phòng HĐND và UBND huyện). Trường hợp có sự cố nghiêm trọng vượt quá khả năng khắc phục của đơn vị thì phải báo cáo cho cơ quan cấp trên quản lý trực tiếp là Sở Thông tin và Truyền thông tỉnh Bình Định để được hướng dẫn, hỗ trợ, phối hợp xử lý.

3. Phối hợp chặt chẽ với cơ quan Công an huyện trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động vi phạm an toàn, an ninh thông tin. 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 triển khai công tác kiểm tra khắc phục sự cố; 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 UBND huyện (qua Văn phòng HĐND và UBND huyện) định kỳ hàng năm (trước ngày 20 tháng 10).

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

1. Trách nhiệm của cán bộ chuyên trách an toàn an ninh thông tin:

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

b) Phối hợp với các cá nhân, đơn vị có liên quan trong việc kiểm tra, phát hiện và khắc phục các sự cố mất an toàn, an ninh thông tin.

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

a) Chấp hành nghiêm túc các quy định về an toàn, an ninh thông tin 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 cơ quan, đơn vị.

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

c) Tích cực tham gia các chương trình đào tạo, hội nghị về an toàn an ninh thông tin do UBND huyện, Sở Thông tin và Truyền thông hoặc các đơn vị chuyên môn tổ chức.

Điều 11. Trách nhiệm của Văn phòng HĐND và UBND huyện:

1. Tham mưu UBND huyện về công tác đảm bảo an toàn, an ninh thông tin trên địa bàn tỉnh và chịu trách nhiệm trước UBND huyện trong việc đảm bảo an toàn an ninh cho các hệ thống thông tin cấp huyện.
2. Hàng năm xây dựng kế hoạch, dự toán nguồn kinh phí để triển khai công tác an toàn và an ninh thông tin phục vụ cho việc vận hành các hệ thống thông tin được UBND huyện giao quản lý.
3. Chủ trì, phối hợp với các cơ quan liên quan thành lập đoàn kiểm tra, tiến hành kiểm tra định kỳ hoặc đột xuất khi phát hiện có các dấu hiệu, hành vi vi phạm an toàn, an ninh thông tin trên địa bàn huyện theo đúng quy định hiện hành.
4. 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 huyện.
5. 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 mất an toàn, an ninh thông tin.
6. Hướng dẫn, giám sát các cơ quan đơn vị trên địa bàn huyện xây dựng quy chế và thực hiện đảm bảo an toàn cho hệ thống thông tin theo quy định của Nhà nước.

Chương IV

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

Điều 12. Kế hoạch kiểm tra hàng năm

1. Văn phòng HĐND và UBND huyện chủ trì, phối hợp với phòng Văn hóa và Thông tin huyện, Công an huyện và các đơn vị có liên quan tiến hành kiểm tra công tác đảm bảo an toàn, an ninh thông tin định kỳ hàng năm đối với các cơ quan, đơn vị cấp huyện, UBND các xã, thị trấn định kỳ hàng năm (tối thiểu 01 lần/năm).
2. Tiến hành kiểm tra đột xuất các cơ quan, đơn vị khi phát hiện có dấu hiệu vi phạm an toàn, an ninh thông tin.

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

1. Phòng Văn hóa và Thông tin huyện:
 - a) Chịu trách nhiệm chủ trì, phối hợp với các cơ quan chức năng liên quan để thành lập Đoàn kiểm tra công tác đảm bảo an toàn, an ninh thông tin, Tổ chức triển khai công tác kiểm tra an toàn, an ninh thông tin trên địa bàn huyện và báo cáo kết quả kiểm tra cho UBND huyện.
 - b) Tiến hành xử phạt theo thẩm quyền các hành vi vi phạm an toàn, an ninh thông tin gây thiệt hại cho hệ thống thông tin các cơ quan nhà nước trên địa bàn huyện.
 - c) Tổ chức và thực hiện tuyên truyền công tác an toàn, an ninh thông tin cho các cơ quan, đơn vị trên địa bàn tỉnh.

2. Công an huyện:

a) Phối hợp phòng Văn hóa và Thông tin, Văn phòng HĐND và UBND huyện 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.

3. Trách nhiệm các cơ quan liên quan:

a) Cử cán bộ chuyên trách tham gia Đoàn kiểm tra, phối hợp với phòng Văn hóa và Thông tin huyện và các đơn vị liên thực hiện việc 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 trên địa bàn tỉnh.

Chương V **TỔ CHỨC THỰC HIỆN**

Điều 14. Khen thưởng và xử lý vi phạm

1. Hàng năm, phòng Văn hóa và Thông tin, Văn phòng HĐND và UBND dựa trên các điều tra, báo cáo công tác an toàn, an ninh thông tin của các cơ quan, đơn vị để lập bảng xếp hạng an toàn, an ninh thông tin, trên cơ sở đó đề xuất UBND huyện xem xét khen thưởng các cơ quan, đơn vị, cá nhân theo quy định hiện hành.

2. Các cơ quan, đơn vị, cá nhân có hành vi vi phạm Quy chế này, tùy theo tính chất, mức độ vi phạm mà bị xử lý theo quy định hiện hành.

Điều 15. Điều khoản thi hành

Phòng Văn hóa và Thông tin huyện chủ trì, phối hợp với Văn phòng HĐND và UBND huyện và các phòng, ban, ngành UBND các xã, thị trấn có trách nhiệm hướng dẫn triển khai thực hiện Quy chế này.

Trong quá trình thực hiện, nếu có vướng mắc, phát sinh, các cơ quan, đơn vị, địa phương kịp thời phản ánh về Văn phòng HĐND và UBND huyện để tổng hợp, báo cáo UBND huyện xem xét sửa đổi, bổ sung cho phù hợp. /s

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



Đỗ Văn Lọt

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 (Ban hành kèm theo Quyết định số 4139 /QĐ-UBND ngày 24/12/2012 của UBND huyện Tây Sơn)

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.

e) Quản trị mạng: Đảm bảo việc an toàn, an ninh 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 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.

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

f) Kiểm soát truy cập ứng dụng: Tránh truy cập trái phép vào hệ thống.

g) Giám sát truy cập 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 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.

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. 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 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

(Ban hành kèm theo Quyết định số 4139 /QĐ-UBND ngày 24/12/2012
của UBND huyện Tây Sơn)

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.