ỦY BAN NHÂN DÂN TỈNH CÀ MAU	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 26 /2016/QĐ-UBND	*Cà Mau, ngày 26 tháng 7 năm 2016*

QUYẾT ĐỊNH
Ban hành Quy chế đảm bảo an toàn thông tin mạng trong hoạt động cơ quan, đơn vị trên địa bàn tỉnh Cà Mau

ỦY BAN NHÂN DÂN TỈNH CÀ MAU

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19 tháng 6 năm 2015;

Căn cứ Luật Công nghệ thông tin ngày 29 tháng 6 năm 2006;

Căn cứ Luật Ban hành văn bản quy phạm pháp luật ngày 22 tháng 6 năm 2015;

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

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

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

Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Tờ trình số 70/TT-STTTT ngày 07 tháng 7 năm 2016 và Báo cáo thẩm định số 209/BC-STP ngày 01 tháng 7 năm 2016 của Giám đốc Sở Tư pháp,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này "Quy chế đảm bảo an toàn thông tin mạng trong hoạt động cơ quan, đơn vị trên địa bàn tỉnh Cà Mau".

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày 01 tháng 8 năm 2016.

Điều 3. 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 Cà Mau và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Văn phòng Chính phủ;
- Bộ Thông tin và Truyền thông (Vụ Pháp chế);
- Cục Kiểm tra văn bản (Bộ Tư pháp);
- TT: Tỉnh ủy, HĐND tỉnh;
- Đoàn đại biểu Quốc hội tỉnh;
- Ủy ban MTTQ VN tỉnh;
- Sở Tư pháp (tự kiểm tra);
- Cổng Thông tin điện tử tỉnh;
- Trung tâm CB-TH;
- Lưu: VT, (TT)-Mi55/7.

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

Thân Đức Hưởng

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

QUY CHẾ
Đảm bảo an toàn thông tin mạng trong hoạt động cơ quan, đơn vị trên địa bàn tỉnh Cà Mau

(Ban hành kèm theo Quyết định số: 26 /2016/QĐ-UBND ngày 26 tháng 7 năm 2016 của Ủy ban nhân dân tỉnh Cà Mau)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định công tác đảm bảo an toàn thông tin, bảo mật trên môi trường mạng trong hoạt động ứng dụng công nghệ thông tin, bao gồm: công tác xây dựng các quy định quản lý đảm bảo an toàn thông tin; việc áp dụng các biện pháp quản lý kỹ thuật, quản lý vận hành đảm bảo an toàn thông tin đối với hệ thống thông tin trên địa bàn tỉnh Cà Mau.

Điều 2. Đối tượng áp dụng

1. Quy chế này được áp dụng đối với các sở, ban, ngành, đoàn thể và các đơn vị sự nghiệp trực thuộc Ủy ban nhân dân tỉnh; các phòng, ban thuộc Ủy ban nhân dân các huyện, thành phố Cà Mau và 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, người lao động đang làm việc trong các cơ quan, đơn vị nêu tại khoản 1 Điều này và các tổ chức, cá nhân có liên quan 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 thông tin

1. Giảm thiểu được các nguy cơ gây sự cố mất an toàn thông tin trong quá trình ứng dụng công nghệ thông tin của cán bộ, công chức, viên chức, người lao động.

2. Công tác đảm bảo an toàn 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 hành chính nhà nước.

3. Các hoạt động ứng dụng công nghệ thông tin phải tuân thủ theo nguyên tắc đảm bảo an toàn thông tin được quy định tại Điều 41 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 cơ quan nhà nước.

Điều 4. Giải thích từ ngữ

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

1. *Mạng:* Là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ, trao đổi thông qua mạng viễn thông và mạng máy tính.

2. *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.

3. *ISO/IEC 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.

4. *ISO/IEC 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.

5. *ISO/IEC 27002:2005:* Tiêu chuẩn quốc tế về một bộ quy định thực thi về quản lý an toàn thông tin.

6. *Hệ thống thông tin:* Là một tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên mạng.

7. *Chủ quản hệ thống thông tin:* Là cơ quan, tổ chức có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin.

8. *Đơn vị vận hành hệ thống thông tin:* Là cơ quan, tổ chức được chủ quản hệ thống thông tin giao nhiệm vụ vận hành hệ thống thông tin.

9. *An toàn thông tin:* 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.

10. *Vi rút máy tính:* Là chương trình máy tính có khả năng lây lan, gây ra hoạt động không bình thường cho thiết bị số hoặc sao chép, sửa đổi, xóa bỏ thông tin lưu trữ trong thiết bị số.

11. *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.

12. *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.

13. *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.

14. *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.

Chương II
QUY ĐỊNH ĐẢM BẢO AN TOÀN THÔNG TIN

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

1. Đối với Thủ trưởng các cơ quan, đơn vị

a) Trang bị đầy đủ các kiến thức bảo mật cơ bản cho cán bộ, công chức, viên chức, người lao động 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, vi rút máy tính trên các máy trạm, máy chủ và các công việc khác có liên quan đến việc bảo đảm an toàn thông tin;

d) Phải bố trí ít nhất 01 máy vi tính riêng, không kết nối mạng nội bộ và mạng Internet dùng để quản lý, soạn thảo các tài liệu mật theo quy định;

đ) 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 chuyên môn và vận hành an toàn hệ thống thông tin của cơ quan, đơn vị, triển khai các biện pháp bảo đảm an toàn thông tin cho tất cả cán bộ, công chức, viên chức, người lao động trong cơ quan, đơn vị mình. Thường xuyên tự nghiên cứu, cập nhật các kiến thức về an toàn thông tin, về nguy cơ tiềm ẩn có thể gây mất thông tin và các biện pháp phòng tránh 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 cho các sản phẩm an toàn thông tin nhưng vẫn duy trì yêu cầu hoạt động bình thường của hệ thống thông tin;

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

đ) Thường xuyên thực hiện việc theo dõi bản ghi nhật ký hệ thống (logfile) 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;

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

3. Đối với cán bộ, công chức, viên chức, người lao động

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

b) Hạn chế việc sử dụng chức năng chia sẻ tài nguyên (sharing), khi sử dụng chức năng này cần bật thuộc tính bảo mật bằng mật khẩu và thực hiện việc 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 những người xâm nhập từ bên ngoài (hacker) 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) Chỉ mở các tập tin đính kèm theo thư điện tử khi biết rõ người gửi thư; phải lưu tập tin vào máy tính rồi quét vi rút trước khi mở; không được mở các thư điện tử có tập tin đính kèm có nguồn gốc không rõ ràng vì rất có thể có vi rút, phần mềm gián điệp được đính kèm theo thư;

đ) Phải đặt mật khẩu truy nhập vào máy tính của mình, đồng thời thiết lập chế độ bảo vệ màn hình (screen saver) có sử dụng mật khẩu bảo vệ sau một khoảng thời gian nhất định không sử dụng máy tính. Sử dụng các thiết bị lưu trữ (USB, ổ cứng gắn ngoài...) an toàn, đúng cách để phòng ngừa vi rút, phần mềm gián điệp xâm nhập máy tính: khi gắn thiết bị lưu trữ vào máy tính, không được trực tiếp truy cập ngay mà phải quét vi rút trước.

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

1. Tổ chức mô hình mạng: Cài đặt, cấu hình, tổ chức hệ thống mạng theo mô hình máy trạm/máy chủ (client/server), hạn chế sử dụng mô hình mạng ngang hàng. Đối với các cơ quan, đơn vị có nhiều phòng, ban, đơn vị trực thuộc không nằm trong cùng một khu vực thì cần thiết lập mạng cục bộ ảo (virtual LAN - VLAN) để tăng cường độ an toàn cho hạ tầng 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), mật khẩu, mã hóa dữ liệu và thông báo các thông tin liên quan đến AP để cơ quan, đơn vị sử dụng, định kỳ 3 tháng 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, sửa đổi, vô hiệu hóa và loại bỏ các tài khoản không còn sử dụng. Đồng thời tổ chức kiểm tra các tài khoản của hệ thống thông tin ít nhất 06 tháng/1 lần và triển khai các công cụ tự động để hỗ trợ việc quản lý các tài khoản của hệ thống thông tin. Hủy tài khoản, quyền truy nhập hệ thống thông tin, thu hồi lại tất cả các tài nguyên liên quan tới hệ thống thông tin (khóa, thẻ nhận dạng, thư mục lưu trữ,...) đối với cán bộ, công chức, viên chức, người lao động đã chuyển công tác, chấm dứt hợp đồng lao động.

4. Quản lý đăng nhập hệ thống: Các hệ thống thông tin cần giới hạn số 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. 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 việc sử dụng mạng riêng ảo (VPN) khi có nhu cầu làm việc từ xa; yêu cầu người sử dụng đặt mật khẩu với độ an toàn cao, giám sát, nhắc nhở khuyến cáo nên thay đổi thường xuyên 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 nhập từ xa.

5. Quản lý bản ghi nhật ký hệ thống (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 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. Chống mã độc, vi rút: Lựa chọn, triển khai các phần mềm chống vi rút, thư rác trên các máy chủ, các thiết bị di động trong mạng và những hệ thống thông tin xung yếu như: Cổng thông tin điện tử, thư điện tử, một cửa điện tử,... để phát hiện, loại trừ những đoạn mã độc hại (virus, trojan, worms,...) và hỗ trợ người sử dụng cài đặt các phần mềm này trên máy trạm. Thường xuyên cập nhật các phiên bản mới, các bản vá lỗi của các phần mềm chống vi rút để bảo đảm chương trình quét vi rút của cơ quan, đơn vị 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 hằng 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 đơn vị trong tổ chức; khuyến cáo người sử dụng 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 việc chia sẻ tài nguyên trên máy chủ hoặc trên máy cục bộ nên 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: 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. Sau khi sao lưu dữ liệu được lưu vào các thiết bị lưu trữ như: CD, ổ cứng gắn ngoài,... và thực hiện việc đánh số, dán nhãn để tránh nhầm lẫn, các thiết bị lưu trữ này được cất giữ ở nơi an toàn, bảo mật nhằm phục vụ cho công tác phục hồi dữ liệu một cách nhanh nhất;

b) Đối với máy chủ: Bảo đảm thiết lập cơ chế sao lưu và phục hồi hệ thống của máy chủ. Tùy thuộc vào hệ điều hành của máy chủ, có thể sử dụng chức năng sẵn có của hệ điều hành hoặc phần mềm phù hợp để sao lưu và khôi phục lại toàn bộ máy chủ hoặc các tập tin, thư mục được lựa chọn.

9. 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 trang chủ bị thay đổi, hệ thống hoạt động rất chậm, khác thường,... cần thực hiện các bước cơ bản sau:

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

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

c) Bước 3: Khôi phục hệ thống bằng cách chuyển dữ liệu dự phòng (backup) mới nhất để hệ thống hoạt động.

10. Hệ thống thông tin cần có cơ chế ngăn chặn hoặc hạn chế các sự cố gây ra do tấn công từ chối dịch vụ (DoS, DDoS). Bố trí thiết bị đặt tại biên của mạng có chức năng 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 7. Xây dựng quy chế nội bộ đảm bảo an toàn 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 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 của hệ thống thông tin sử dụng các biện pháp trong Điều 5 và Điều 6 của Quy chế này;

e) Nguyên tắc chung 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 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 thông tin cho đơn vị cần căn cứ các tiêu chuẩn kỹ thuật quản lý an toàn của bộ tiêu chuẩn ISO/IEC 17799:2005 hoặc ISO/IEC 27002:2005 để áp dụng phù hợp với cơ quan, đơn vị mình.

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

1. Các cơ quan, đơn vị phải xây dựng và áp dụng quy trình đảm bảo an toàn cho hệ thống thông tin của mình 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 sau:

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

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

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

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

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

2. Các cơ quan, đơn vị tham khảo các bước cơ bản để xây dựng khung quy trình đảm bảo an toàn thông tin cho hệ thống thông tin theo tiêu chuẩn quốc tế ISO/IEC 27001:2005.

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN

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

1. Thủ trưởng các cơ quan, đơn vị có trách nhiệm tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trước Ủy ban nhân dân tỉnh, Chủ tịch Ủy ban nhân dân tỉnh trong công tác bảo vệ an toàn thông tin mạng của cơ quan, đơn vị.

2. Khi hệ thống thông tin bị gây nguy hại ảnh hưởng đến tính nguyên vẹn, tính bảo mật hoặc tính khả dụng của thông tin phải kịp thời áp dụng mọi biện pháp để khắc phục và hạn chế thiệt hại, ưu tiên sử dụng lực lượng kỹ thuật an toàn thông tin 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 hệ thống thông tin bị gây nguy hại ảnh hưởng đến tính nguyên vẹn, tính bảo mật hoặc tính khả dụng của thông tin vượt quá khả năng khắc phục của cơ quan, đơn vị thì 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, phối hợp xử lý.

3. Phối hợp chặt chẽ với cơ quan Công an trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn 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. Cử cán bộ chuyên trách công nghệ thông tin, phối hợp với cơ quan chuyên trách công nghệ thông tin để 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 cơ quan chuyên trách công nghệ thông tin yêu cầu.

5. Định kỳ hàng năm phải báo cáo tình hình và kết quả thực hiện công tác đảm bảo an toàn thông tin tại cơ quan, đơn vị và gửi về Sở Thông tin và Truyền thông (trước ngày 20 tháng 12).

6. Phối hợp xây dựng các tiêu chí và quy trình kỹ thuật kiểm tra công tác đảm bảo an toàn thông tin.

Điều 10. Trách nhiệm của Sở Thông tin và Truyền thông

1. Giúp UBND tỉnh quản lý về công tác đảm bảo an toàn thông tin mạng trên địa bàn tỉnh và chịu trách nhiệm trước UBND tỉnh, Chủ tịch UBND tỉnh trong việc đảm bảo an toàn cho các hệ thống thông tin cấp tỉnh.

2. Hằng năm xây dựng kế hoạch, dự toán nguồn kinh phí để triển khai công tác an toàn thông tin phục vụ cho việc vận hành các hệ thống thông tin được UBND tỉnh giao quản lý.

3. Chủ trì, phối hợp với các cơ quan liên quan tổ chức kiểm tra công tác đảm bảo an toàn thông tin theo định kỳ hoặc kiểm tra đột xuất khi phát hiện có các dấu hiệu, hành vi vi phạm an toàn thông tin trên địa bàn tỉnh theo đúng quy định hiện hành, báo cáo kết quả kiểm tra cho Ủy ban nhân dân tỉnh.

4. Xử lý theo thẩm quyền các hành vi vi phạm an toàn thông tin gây thiệt hại cho hệ thống thông tin của các cơ quan, đơn vị trên địa bàn tỉnh.

5. Xây dựng và triển khai các chương trình đào tạo, hội nghị tuyên truyền về an toàn thông tin trên địa bàn tỉnh.

6. Chỉ đạo các cơ quan báo, đài tuyên truyền công tác đảm bảo an toàn thông tin tại các cơ quan, đơn vị trên địa bàn tỉnh.

7. Tùy theo mức độ sự cố, phối hợp với 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 thông tin.

8. Hướng dẫn, giám sát các cơ quan, đơn vị trên địa bàn tỉnh xây dựng quy chế và thực hiện việc đảm bảo an toàn cho hệ thống thông tin theo quy định của Nhà nước.

Điều 11. Trách nhiệm của cán bộ, công chức, viên chức, người lao động trong các cơ quan, đơn vị

1. Trách nhiệm của cán bộ chuyên trách an toàn hệ thống thông tin

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

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

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

a) Nghiêm chỉnh chấp hành các quy chế nội bộ, quy trình về an toàn 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 toàn thông tin tại cơ quan, đơn vị;

b) Khi phát hiện sự cố phải báo cáo ngay với lãnh đạo cơ quan, đơn vị và bộ phận chuyên trách để kịp thời ngăn chặn, xử lý;

c) Tham gia các chương trình đào tạo, hội nghị, hội thảo về an toàn thông tin do Sở Thông tin và Truyền thông hoặc các cơ quan chuyên môn tổ chức.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 12. Điều khoản thi hành

1. Sở Thông tin và Truyền thông chủ trì, phối hợp với các sở, ban, ngành, đoàn thể cấp tỉnh, Ủy ban nhân dân các huyện, thành phố Cà Mau và các cơ quan, đơn vị có liên quan triển khai thực hiện Quy chế này.

2. Trong quá trình thực hiện, nếu có khó khăn, vướng mắc; các cơ quan, đơn vị phản ánh bằng văn bản về Sở Thông tin và Truyền thông để tổng hợp, báo cáo Ủy ban nhân dân tỉnh xem xét sửa đổi, bổ sung Quy chế này cho phù hợp với quy định của pháp luật hiện hành và tình hình thực tế của địa phương./.

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

Thân Đức Hưởng