ỦY BAN NHÂN DÂN HUYỆN TỊNH BIÊN	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 01 /2019/QĐ-UBND	*Tịnh Biên, ngày 16 tháng 7 năm 2019*

QUYẾT ĐỊNH

Ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan Nhà nước trên địa bàn huyện Tịnh Biên

ỦY BAN NHÂN DÂN HUYỆN TỊNH BIÊN

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

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

Căn cứ Luật Giao dịch Điện tử ngày 29/11/2005;

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

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

Căn cứ Luật An ninh mạng ngày 12/6/2018;

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

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Nghị định số 142/2016/NĐ-CP ngày 14/10/2016 của Chính phủ về ngăn chặn xung đột thông tin trên mạng;

Căn cứ Thông tư số 27/2011/TT-BTTTT ngày 04/10/2011 của Bộ Thông tin và Truyền thông quy định về điều phối các hoạt động ứng cứu sự cố mạng Internet Việt Nam;

Căn cứ Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ trưởng Bộ Thông tin và Truyền thông về Quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định số 67/2017/QĐ-UBND, ngày 04/10/2017 của UBND tỉnh về việc Ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh An Giang;

Căn cứ Kế hoạch số 74/KH-UBND ngày 22/3/2019 của UBND huyện Tịnh Biên về ứng dụng công nghệ thông tin trong hoạt động của cơ quan Nhà nước năm 2019 trên địa bàn huyện Tịnh Biên;

Xét Đề nghị của Phòng Văn hóa và Thông tin tại Tờ trình số 54/TTr-PVHTT ngày 10/7/2019,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn huyện Tịnh Biên.

Điều 2. Quyết định này có hiệu lực thi hành sau 07 ngày, kể từ ngày ký ban hành.

Điều 3. Chánh Văn phòng UBND huyện, Thủ trưởng các ban, ngành huyện, Chủ tịch UBND các xã, thị trấn và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Văn phòng UBND tỉnh;
- Sở Thông tin và Truyền thông;
- TT. Huyện ủy;
- TT. HĐND huyện;
- LĐ. UBND huyện;
- Phòng ban ngành huyện;
- UBND 14 xã, thị trấn;
- Lưu: VT, VX.

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

Trần Bá Phước

ỦY BAN NHÂN DÂN HUYỆN TỊNH BIÊN	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc

QUY CHẾ
Về đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin trong hoạt động của các cơ quan Nhà nước trên địa bàn huyện Tịnh Biên

(Ban hành kèm theo Quyết định số 01/2019/QĐ-UBND Ngày 16 tháng 7 năm 2019 của Ủy ban nhân dân huyện)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. 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 của các cơ quan nhà nước, đơn vị sự nghiệp trên địa bàn huyện Tịnh Biên (sau đây gọi tắt là cơ quan).

2. Quy chế này được áp dụng đối với UBND huyện; UBND các xã, thị trấn; Đơn vị sự nghiệp của trên địa bàn huyện; Cán bộ, công chức, viên chức, người lao động (gọi tắt là cán bộ, công chức) và các tổ chức, cá nhân có liên quan tham gia vận hành, khai thác các hệ thống thông tin tại cơ quan trên địa bàn huyện Tịnh Biên.

Điều 2. Mục đích, nguyên tắc đảm bảo an toàn, an ninh thông tin

1. Việc áp dụng Quy chế này nhằm giảm thiểu được các nguy cơ gây mất an toàn thông tin và đảm bảo an ninh thông tin trong quá trình ứng dụng công nghệ thông tin trong hoạt động của các cơ quan.

2. Các hoạt động ứng dụng công nghệ thông tin phải tuân theo nguyên tắc đảm bảo an toàn thông tin được quy định tại Điều 41, 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.

Chương II
QUY ĐỊNH ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 3. Bảo vệ thông tin cá nhân

Cán bộ, công chức có trách nhiệm tự bảo vệ thông tin cá nhân của mình. Khi sử dụng, khai thác các hệ thống thông tin, các phần mềm ứng dụng trong hoạt động Nhà nước, có trách nhiệm:

a. Tự quản lý máy tính và các dữ liệu cá nhân.

b. Tự quản lý các tài khoản không tiết lộ mật khẩu đăng nhập, truy cập trái phép vào hệ thống dữ liệu.

c. Khi khai thác, sử dụng các phần mềm trong hệ thống Nhà nước tại các điểm truy cập internet công cộng, tuyệt đối không đặt chế độ lưu trữ mật khẩu trong quá trình sử dụng.

Điều 4. Về quản lý cán bộ, công chức và viên chức và người lao động

1. Các cơ quan phải thường xuyên tổ chức quán triệt các quy định về an toàn thông tin, nhằm nâng cao nhận thức về trách nhiệm đảm bảo an toàn thông tin của từng cá nhân trong cơ quan.

2. Phân công cán bộ, công chức chuyên trách hoặc phụ trách CNTT, để quản lý kỹ thuật nghiệp vụ về an toàn thông tin tại đơn vị;

3. Thủ trưởng cơ quan, đơn vị tạo điều kiện để cán bộ, công chức chuyên trách hoặc phụ trách CNTT học tập, tiếp thu công nghệ, kiến thức an toàn thông tin;

4. Hủy tài khoản, quyền truy cập các hệ thống thông tin, thu hồi lại tất cả các tài sản liên quan tới hệ thống thông tin (khoá, thẻ nhận dạng, thư mục lưu trữ, thư điện tử, máy vi tính, ...) đối với các cá nhân nghỉ việc, chuyển công tác.

Điều 5. Quản lý phòng máy chủ

1. Phải được bố trí ở khu vực có điều kiện an ninh tốt; khô ráo, có điều hòa không khí; nguồn cung cấp điện ổn định và có nguồn điện dự phòng; có bình chữa cháy hoặc hệ thống tự động cảnh báo; phòng, chống sét; Phải thiết lập cơ chế bảo vệ mạng nội bộ, đảm bảo an toàn thông tin khi có kết nối với mạng ngoài bằng các công cụ, thiết bị bảo vệ (tường lửa, hệ thống chống xâm nhập trái phép, hệ thống giám sát, cảnh báo).

2. Các thiết bị phần cứng, phần mềm và cơ sở dữ liệu quan trọng phải được đặt trong phòng máy chủ và có các biện pháp bảo vệ, ngăn chặn xâm nhập trái phép vào phòng máy chủ.

3. Phòng máy chủ của các cơ quan là khu vực hạn chế tiếp cận và được lắp đặt hệ thống camera giám sát. Chỉ những người có trách nhiệm theo quy định của thủ trưởng cơ quan mới được phép vào phòng máy chủ.

4. Quá trình vào, ra phòng máy chủ cử cán bộ thường xuyên kiểm tra, giám sát hệ thống thiết bị, hạ tầng phòng máy chủ phải được ghi nhận vào nhật ký quản lý phòng máy chủ.

Điều 6. Phòng chống mã độc

1. Tất cả các máy trạm, máy chủ phải được trang bị phần mềm phòng chống mã độc. Các phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc.

2. Các cán bộ, công chức và viên chức trong cơ quan phải được hướng dẫn về phòng chống mã độc, các rủi ro do mã độc gây ra; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm trên máy trạm khi chưa có sự đồng ý của người có thẩm quyền theo quy định của cơ quan.

3. Tất cả các máy tính của đơn vị phải được cấu hình nhằm vô hiệu hóa tính năng tự động thực thi (autoplay) các tập tin trên các thiết bị lưu trữ di động.

4. Tất cả các tập tin, thư mục phải được quét mã độc trước khi sao chép, sử dụng.

5. Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm mã độc trên máy trạm (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu,...), người sử dụng phải tắt máy và báo trực tiếp cho bộ phận có trách nhiệm của đơn vị để xử lý.

Điều 7. Sao lưu dữ liệu dự phòng

1. Các dữ liệu quan trọng của cơ quan phải được sao lưu định kỳ, bao gồm: thông tin cấu hình của hệ thống mạng, máy chủ; phần mềm ứng dụng và cơ sở dữ liệu; tập tin ghi nhật ký.

2. Các cơ quan phải lập kế hoạch và thực hiện sao lưu dữ liệu định kỳ phù hợp với điều kiện của từng cơ quan, đảm bảo khả năng phục hồi dữ liệu khi có sự cố xảy ra.

Điều 8. Quản lý thiết bị tường lửa

1. Các hạ tầng công nghệ thông tin phải được trang bị tường lửa để ngăn chặn và phát hiện các xâm nhập trái phép vào mạng nội bộ.

2. Không được tự ý điều chỉnh thay đổi cấu hình tường lửa khi chưa có sự đồng ý của bộ phận chuyên môn.

3. Nhật ký hoạt động của thiết bị tường lửa phải được lưu giữ an toàn để phục vụ công tác khảo sát, điều tra khi có sự cố xảy ra.

Điều 9. Quản lý truy cập

Mỗi cán bộ, công chức và viên chức chỉ được phép truy cập các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình, có trách nhiệm bảo mật tài khoản truy cập thông tin.

1. Các hệ thống thông tin cần giới hạn số lần đăng nhập sai liên tiếp vào hệ thống. Hệ thống tự động khoá tài khoản trong một khoảng thời gian nhất định trước khi tiếp tục cho đăng nhập lại. Nếu liên tục đăng nhập sai 5 lần vượt quá số lần quy định khóa luôn.

2. Tất cả máy trạm, máy chủ phải được đặt mật khẩu khi vào truy cập.

3. Khi thiết lập mạng không dây trong nội bộ cơ quan, đơn vị, phải đặt mật khẩu truy cập vào mạng không dây.

4. Mật khẩu đăng nhập vào các hệ thống thông tin phải có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự số và ký tự đặc biệt như !, @, #, $, %,...) và phải được thay đổi ít nhất 3 tháng/lần.

Điều 10. Quản lý sự cố

Phân loại mức độ nghiêm trọng của các sự cố, bao gồm:

a) Thấp: sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của cơ quan;

b) Trung bình: sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hay đình trệ hoạt động chính của đơn vị;

c) Cao: sự cố làm cho thiết bị, phần mềm hay hệ thống không thể sử dụng được và gây ảnh hưởng đến một trong các hoạt động chính của cơ quan;

d) Khẩn cấp: sự cố ảnh hưởng đến sự liên tục của nhiều hoạt động chính của cơ quan.

Khi có sự cố hoặc nguy cơ mất an toàn thông tin thì lãnh đạo cơ quan, đơn vị phải chỉ đạo kịp thời để khắc phục và hạn chế thiệt hại, báo cáo bằng văn bản cho cơ quan cấp trên trực tiếp quản lý và Phòng Văn hóa và Thông tin hoặc Văn phòng HĐND và UBND huyện.

Trường hợp có sự cố nghiêm trọng ở mức độ cao, khẩn cấp hoặc vượt quá khả năng khắc phục của cơ quan, đơn vị, lãnh đạo cơ quan, đơn vị phải báo cáo ngay cho cơ quan cấp trên quản lý trực tiếp và Phòng Văn hóa và Thông tin hoặc Văn phòng HĐND và UBND huyện để được hướng dẫn, hỗ trợ kịp thời.

Điều 11. Các hành vi bị nghiêm cấm

1. Cài đặt thêm các chương trình, phần mềm không rõ nguồn gốc, can thiệp vào phần cứng và phầm mềm cài đặt sẵn, tự ý dịch chuyển, tháo lắp các trang thiết bị mà không có sự đồng ý của cấp có thẩm quyền;

2. Không tự ý lắp đặt thêm các thiết bị mạng: Router, Modem, Access Point, Modem Router…Khi chưa có sự đồng ý của bộ phận chuyên môn.

3. Không tự ý thay đổi cấu hình thiết bị mạng.

4. Xâm nhập trái phép, thay đổi, xóa cơ sở dữ liệu của cơ quan Nhà nước.

5. Sử dụng không gian mạng cho mục đích trái pháp luật theo Điều 8 của Luật An ninh mạng.

6. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của cơ quan, cá nhân khác trên môi trường mạng.

7. Hành vi khác làm mất an toàn, bí mật thông tin của cơ quan, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

Điều 12. Tiếp nhận thông tin báo cáo sự cố mất an toàn thông tin trên địa bàn huyện

Địa chỉ tiếp nhận thông tin, báo cáo sự cố mất an toàn thông tin trên địa bàn huyện Tịnh Biên: (Phân loại sự cố theo điều 10) Sự cố tắc, nghẽn, đứt, rớt, không truy cập được mạng, phần mềm trong hoạt động Nhà nước, máy tính bị mã hóa dữ liệu. Các đơn vị báo về Phòng Văn hóa và Thông tin hoặc Văn phòng UBND (hoặc Tổ ứng cứu thông tin nếu có) để được hỗ trợ, hướng dẫn khắc phục.

Điện thoại: 02963 875 486. Email:pvhtt.tinhbien@angiang.gov.vn

Chương III

TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 13. Trách nhiệm của cán bộ, công chức và viên chức trong các cơ quan

1. Trách nhiệm của cán bộ, công chức, viên chức phụ trách an toàn thông tin:

a) Chịu trách nhiệm đảm bảo an toàn thông tin của đơn vị;

b) Tham mưu lãnh đạo cơ quan ban hành các quy định, quy trình nội bộ, triển khai các giải pháp kỹ thuật đảm bảo an toàn thông tin;

c) Thực hiện việc giám sát, đánh giá, báo cáo thủ trưởng cơ quan các rủi ro mất an toàn thông tin và mức độ nghiêm trọng của các rủi ro đó;

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

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

a) Nghiêm túc chấp hành các quy định, quy trình nội bộ, Quy chế này và các quy định khác của pháp luật về an toàn thông tin. Chịu trách nhiệm đảm bảo an toàn thông tin trong phạm vi trách nhiệm và quyền hạn được giao;

b) Mỗi cán bộ, công chức và viên chức phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp các thiết bị trên máy tính; không được truy cập vào các trang web không rõ về nội dung; không tải và cài đặt các phần mềm không rõ nguồn gốc, không liên quan đến công việc chuyên môn; không nhấp chuột vào các đường dẫn lạ không rõ về nội dung;

c) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin phải báo cáo ngay với cấp trên và bộ phận chuyên trách công nghệ thông tin của đơn vị để kịp thời ngăn chặn và xử lý;

d) Tham gia các chương trình đào tạo, hội nghị về an toàn an ninh thông tin do cơ quan hoặc Phòng Văn hóa và Thông tin tổ chức.

Điều 14. Trách nhiệm của 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 UBND huyện trong công tác đảm bảo an toàn thông tin của đơn vị mình.

2. Phân công một bộ phận hoặc cán bộ chuyên trách đảm bảo an toàn thông tin của đơn vị; tạo điều kiện để các cán bộ phụ trách an toàn thông tin được học tập, nâng cao trình độ chuyên môn về an toàn thông tin.

3. Xây dựng quy định, quy trình nội bộ về đảm bảo an toàn thông tin phù hợp với Quy chế này và các quy định của pháp luật.

4. Phối hợp, cung cấp thông tin và tạo điều kiện cho các đơn vị có thẩm quyền triển khai công tác kiểm tra khắc phục sự cố xảy ra một cách kịp thời, nhanh chóng và đạt hiệu quả.

5. Phối hợp chặt chẽ với Công an huyện trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn, an ninh thông tin.

6. Định kỳ hàng quý, các cơ quan lập báo cáo về tình hình an toàn thông tin và gửi về Phòng Văn hóa và Thông tin để tổng hợp báo cáo UBND huyện.

Điều 15. Trách nhiệm của Phòng Văn hóa và Thông tin

1. Tham mưu UBND huyện về công tác đảm bảo an toàn, an ninh thông tin trên địa bàn huyện và chịu trách nhiệm trước UBND huyện trong việc đảm bảo an toàn an ninh cho các hệ thống thông tin của huyện.

2. Hàng năm xây dựng kế hoạch triển khai công tác đảm bảo an toàn 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 Công an huyện và các cơ quan, đơn vị liên quan tổ chức kiểm tra theo định kỳ hoặc đột xuất; kịp thời phát hiện và xử lý theo quy định của pháp luật đối với các cơ quan, tổ chức, cá nhân có các dấu hiệu, hành vi vi phạm an toàn, an ninh thông tin trên địa bàn huyện.

4. Hàng năm xây dựng và triển khai các chương trình đào tạo chuyên sâu về an toàn, an ninh thông tin cho lực lượng đảm bảo an toàn, an ninh thông tin của các cơ quan, đơn vị.

5. Tổ chức các hội nghị, hội thảo chuyên đề và tuyên truyền về an toàn, an ninh thông tin trong công tác quản lý Nhà nước trên địa bàn huyện.

6. Tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin.

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

8. Tổng hợp và báo cáo về tình hình an toàn, an ninh thông tin theo định kỳ cho Phòng Văn hóa và Thông tin.

Điều 16. Trách nhiệm của Công an huyện

1. Chủ trì, phối hợp với Phòng Văn hóa và Thông tin và các cơ quan, đơn vị có liên quan xây dựng kế hoạch và chịu trách nhiệm kiểm soát, phòng ngừa, đấu tranh, ngăn chặn các loại tội phạm lợi dụng hệ thống thông tin gây hại đến an toàn, an ninh thông tin trong cơ quan nhà nước.

2. Phối hợp với các cơ quan chức năng trong trao đổi biện pháp kỹ thuật, kiểm tra, đánh giá nhằm đảm bảo an toàn, an ninh thông tin.

3. Tăng cường công tác phòng ngừa, phát hiện và tuyên truyền, phổ biến pháp luật về xử lý tội phạm trong việc đảm bảo an toàn, an ninh thông tin.

4. Điều tra và xử lý các trường hợp vi phạm pháp luật về an toàn, an ninh thông tin theo thẩm quyền.

5. Thực hiện nhiệm vụ bảo vệ an toàn các công trình quan trọng về an ninh quốc gia trên lĩnh vực công nghệ thông tin.

6. Bảo đảm các yêu cầu về an toàn thông tin theo quy định của Điều 11 Quy chế này.

Chương IV

TỔ CHỨC THỰC HIỆN

Điều 17. Khen thưởng và xử lý vi phạm

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

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

Điều 18. Thủ trưởng các cơ quan, đơn vị trên địa bàn huyện chịu trách nhiệm tổ chức triển khai thực hiện Quy chế tại đơn vị mình.

Điều 19. Phòng Tài chính và Kế hoạch phối hợp Phòng Văn hóa và Thông tin ưu tiên bố trí kinh phí thực hiện các nhiệm vụ đảm bảo an toàn thông tin của huyện.

Điều 20.Trong quá trình thực hiện, nếu có những vấn đề cần sửa đổi, bổ sung, đề nghị các đơn vị gửi về Phòng Văn hóa và Thông tin để tổng hợp, báo cáo UBND huyện xem xét, quyết định./.

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

Trần Bá Phước