ỦY BAN NHÂN DÂN HUYỆN CHÂU THÀNH	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 678/QĐ-UBND	*Châu Thành, ngày 10 tháng 3 năm 2015*

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 nhà nước, đơn vị sự nghiệp, Ủy ban nhân dân các xã, thị trấn trên địa bàn huyện Châu Thành

CHỦ TỊCH ỦY BAN NHÂN DÂN HUYỆN

Căn cứ Luật Tổ chức Hội đồng nhân dân và Ủy ban nhân dân năm 2003;

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

Căn cứ Pháp lệnh Bảo vệ bí mật nhà nước số 30/2000/PL-UBTVQH ngày 28 tháng 12 năm 2000 của Ủy ban thường vụ Quốc hội;

Căn cứ Chỉ thị số 28-CT/TW ngày 16 tháng 9 năm 2013 của Ban Bí thư Trung ương Đảng về tăng cường công tác đảm bảo an toàn thông tin mạng;

Căn cứ Nghị định số 26/2007/NĐ-CP ngày 15 tháng 02 năm 2007 của Chính phủ Quy định chi tiết thi hành Luật Giao dịch điện tử về chữ ký số và dịch vụ chữ ký số;

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

Căn cứ Nghị định số 72/2013/NĐ-CP ngày 15 tháng 7 năm 2013 của Chính phủ về việc Quản lý, cung cấp, sử dụng, dịch vụ Internet và thông tin trên mạng;

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 61/2014/QĐ-UBND ngày 11/11/2014 của Ủy ban nhân dân tỉnh về việc Ban hành Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Tây Ninh;

Xét đề nghị của Chánh Văn phòng Hội đồng nhân dân và Ủy ban nhân dân 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 nhà nước, đơn vị sự nghiệp, Ủy ban nhân dân các xã, thị trấn trên địa bàn huyện Châu Thành.

Điều 2. Quyết định này có hiệu lực kể từ ngày ký.

Điều 3. Các cơ quan chuyên môn và đơn vị sự nghiệp, cán bộ, công chức, viên chức và người lao động thuộc Ủy ban dân huyện và Ủy ban dân dân các xã, thị trấn trên địa bàn huyện chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Sở TTTT;
- TT HU, HĐND;
- CT, PCT UBND huyện;
- Như điều 3;
- Lưu: VT.

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Đã ký

Nguyễn Thanh Lam

ỦY BAN NHÂN DÂN
HUYỆN CHÂU THÀNH

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

QUY CHẾ
Đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan Quản lý nhà nước, đơn vị sự nghiệp, Ủy ban nhân dân các xã, thị trấn trên địa bàn huyện Châu Thành

(Ban hành kèm theo Quyết định số 678/QĐ -UBND ngày 10/3/2015 của Chủ tịch UBND huyện Châu Thành)

Chương I
NHỮNG QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định các nội dung, biện pháp đảm bảo an toàn, an ninh thông tin (viết tắt là AT-ANTT) trong lĩnh vực ứng dụng công nghệ thông tin (viết tắt là CNTT) phục vụ cho công tác điều hành và quản lý nhà nước của các cơ quan quản lý nhà nước (viết tắt là QLNN) thuộc Ủy ban nhân dân (viết tắt là UBND) huyện, đơn vị sự nghiệp trực thuộc UBND huyện, UBND các xã, thị trấn trên địa bàn huyện Châu Thành.

Điều 2. Đối tượng áp dụng

Quy chế này áp dụng đối với cán bộ, công chức, viên chức, người lao động (viết tắt là CBCCVC) trong các cơ quan, đơn vị thuộc UBND huyện, các đơn vị sự nghiệp thuộc cơ quan QLNN của UBND huyện, UBND các xã, thị trấn trên địa bàn

huyện.

Điều 3. Giải thích từ ngữ

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

1. 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.

2. An ninh thông tin: Là việc bảo đảm thông tin trên mạng không gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

3. Hệ thống mạng LAN: Là hệ thống mạng nội bộ dùng để kết nối các máy tính trong một phạm vi nhỏ *(nhà ở, phòng làm việc, trường học,...)*. Các máy tính trong mạng LAN có thể chia sẻ tài nguyên với nhau, mà điển hình là chia sẻ tập tin, máy in, máy quét và một số thiết bị khác.

4. Địa chỉ IP: Là một địa chỉ đơn nhất mà những thiết bị điện tử hiện nay đang sử dụng để nhận diện và liên lạc với nhau trên mạng máy tính bằng cách sử dụng giao thức Internet.

5. Thiết bị lưu trữ ngoài: Là các ổ cứng di động, USB, đĩa CD, DVD,…

*6. Hacker***:** Là người có thể viết hay chỉnh sửa phần mềm, phần cứng máy tính bao gồm lập trình, quản trị và bảo mật. Những người này hiểu rõ hoạt động của hệ thống máy tính, mạng máy tính và dùng kiến thức của bản thân để làm thay đổi, chỉnh sửa nó với nhiều mục đích tốt xấu khác nhau.

Chương II
QUY ĐỊNH ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 4. Bộ phận phụ trách đảm bảo an toàn, an ninh thông tin

1. Văn phòng HĐND và UBND huyện là cơ quan trực tiếp chủ trì, phối hợp với các cơ quan liên quan tham mưu cho UBND huyện về công tác quản lý và đảm bảo AT-ANTT trong ứng dụng CNTT trên địa bàn.

2. UBND huyện bố trí 01 công chức phụ trách CNTT chuyên trách biên chế tại Văn phòng HĐND và UBND huyện.

3. Mỗi cơ quan, đơn vị, Ủy ban nhân các xã, thị trấn bố trí ít nhất 01 cán bộ kiêm nhiệm phụ trách CNTT của cơ quan, đơn vị mình.

Điều 5. Quản lý tài khoản người dùng

1. Cán bộ phụ trách CNTT của huyện có trách nhiệm phối hợp với cán bộ CNTT của Văn phòng HĐND - UBND huyện tạo lập và cung cấp tài khoản truy nhập tài khoản người dùng cho CBCCVC của huyện; tạo mới hoặc hủy bỏ tài

khoản của CBCCVC theo Quyết định điều động, bổ nhiệm luân chuyển, nghỉ công tác tại huyện.

2. CBCCVC phải cài đặt mật khẩu cho máy tính cá nhân của mình, có trách nhiệm bảo vệ và bảo mật tài khoản, dữ liệu của cá nhân, của phòng và của cơ quan như: Hòm thư công vụ, phần mềm Quản lý văn bản và Điều hành công việc Eoffice *(viết tắt là QLVB&ĐHCV),* phần mềm Một cửa điện tử, …; không tự ý xâm nhập các tài khoản của người khác để sử dụng; không cung cấp thông tin tài khoản của cá nhân, cơ quan cho các tổ chức, cá nhân không có liên quan.

Mật khẩu phải thay đổi thường xuyên hoặc định kỳ mỗi 03 tháng 01 lần; không dùng một mật khẩu trong nhiều tài khoản.

Điều 6. Về quản lý, sử dụng cơ sở vật chất

1. Đối với thiết bị CNTT

a) CBCCVC có trách nhiệm quản lý trang thiết bị CNTT (máy vi tính, máy in, thiết bị ngoại vi,…) được giao sử dụng, tự quản lý dữ liệu trên máy tính của cá nhân, tự quyết định việc chia sẻ tài nguyên với các máy tính khác theo đúng quy định. Đối với cơ sở dữ liệu thuộc dạng tài liệu "mật" theo quy định khi chia sẻ, cung cấp phải có ý kiến của lãnh đạo cơ quan, đơn vị và được lưu trữ theo quy định của UBND huyện Châu Thành.

b) Cán bộ phụ trách CNTT của huyện và các cán bộ kiêm nhiệm CNTT của các cơ quan, đơn vị, UBND các xã, thị trấn chịu trách nhiệm kiểm tra, theo dõi, đánh giá sự hoạt động của máy chủ, máy trạm, các thiết bị mạng và các thiết bị ngoại vi theo đúng tiêu chuẩn kỹ thuật; thực hiện việc sao lưu dữ liệu thường xuyên; các thiết bị CNTT phải thực hiện công tác bảo trì, bảo dưỡng định kỳ, đột xuất, giảm thiểu tối đa các sự cố kỹ thuật.

c) Máy vi tính chứa dữ liệu quan trọng và thường xuyên kết nối Internet phải cài đặt các phần mềm diệt virus; có cơ chế bảo vệ thư mục và tập tin khi chia sẻ tài nguyên dùng chung.

d) Máy tính và các thiết bị CNTT để nơi an toàn, tránh ảnh hưởng của các tác nhân bên ngoài như nắng, mưa…; không để các tài liệu, vật liệu dễ cháy gần máy tính và các thiết bị CNTT để tránh xảy ra cháy nổ; thường xuyên vệ sinh cho máy vi tính; hàng ngày kiểm tra theo dõi sự hoạt động của máy vi tính và các thiết bị... Khi không sử dụng nên tắt máy vi tính và các thiết bị nhằm tiết kiệm điện và phòng, chống các xâm nhập trái phép.

e) Trong quá trình sử dụng các thiết bị CNTT, khi có sự cố xảy ra đối với các thiết bị CNTT của CBCCVC, người sử dụng thiết bị CNTT thông báo với cán bộ phụ trách CNTT của cơ quan, đơn vị; nếu sự cố nhỏ, không phải thay thế hoặc sửa chữa linh kiện thì cán bộ được giao phụ trách CNTT của cơ quan, đơn vị xử lý trực tiếp. Nếu có sự cố lớn, cần phải sửa chữa, thay thế linh kiện thì người dùng các thiết bị CNTT phải sao lưu dữ liệu, xóa toàn bộ dữ liệu trong các thiết bị lưu trữ trước khi gửi đi sửa chữa. Có thể tham vấn Văn phòng HĐND và UBND huyện để được hướng dẫn sửa chữa, thay thế thiết bị CNTT, tuyệt đối không được chuyển

cho các tập thể, cá nhân chưa được cơ quan có thẩm quyền xác nhận tính an toàn, bảo mật thông tin khi sửa chữa.

2. Hệ thống mạng LAN

a) CBCCVC của cơ quan, đơn vị khi tham gia vào mạng LAN không được tự ý thay đổi các tham số mạng, nếu tự ý thay đổi thông số mạng thì người thay đổi phải chịu hoàn toàn trách nhiệm. Trường hợp cần thiết phải thay đổi tham số mạng, báo cán bộ phụ trách CNTT của cơ quan biết để xử lý.

b) Cán bộ phụ trách CNTT chịu trách nhiệm kiểm tra, theo dõi, đánh giá sự hoạt động của máy chủ, máy trạm, các thiết bị mạng và các thiết bị khác theo đúng tiêu chuẩn kỹ thuật; thực hiện công tác bảo trì, bảo dưỡng định kỳ, đột xuất, giảm tối đa các sự cố kỹ thuật; cung cấp địa chỉ IP mạng và tham số mạng cho người dùng kết nối vào mạng LAN của cơ quan.

c) Cán bộ phụ trách CNTT chịu trách nhiệm hướng dẫn, cài đặt hệ thống an ninh mạng theo đúng tiêu chuẩn an toàn bảo mật; thường xuyên kiểm tra, quét virus cho tất cả các máy tính, xử lý khắc phục kịp thời khi xảy ra sự cố, đảm bảo hệ thống mạng máy tính hoạt động ổn định, liên tục.

d) Hàng năm cán bộ phụ trách CNTT đề xuất kế hoạch mua sắm các thiết bị CNTT để đảm bảo an toàn cho các máy tính và mạng máy tính của cơ quan, đơn vị mình.

Điều 7. Cơ chế sao lưu dữ liệu

1. Phân loại dữ liệu sao lưu

a) Dữ liệu hệ thống bao gồm các loại thông tin, dữ liệu cài đặt như: Cấp phát tài khoản và địa chỉ IP mạng, đưa thông tin lên Trang thông tin điện tử của huyện,...

b) Dữ liệu các ứng dụng dùng chung được cài đặt tại Văn phòng HĐND và UBND huyện như: Phần mềm Eoffice, phần mềm Một cửa điện tử,...

c) Các dữ liệu khác cài đặt trên máy tính cá nhân do các CBCCVC thuộc các cơ quan, đơn vị soạn thảo, tạo lập trên các máy tính trong mạng nội bộ.

2. Quy định thiết bị sao lưu

a) Đối với dữ liệu hệ thống: Sử dụng chức năng sao lưu dự phòng của các ứng dụng.

b) Đối với các dữ liệu khác: Các dữ liệu cần lưu trữ, các cơ quan, đơn vị, UBND các xã, thị trấn tự sao chép vào các thiết bị lưu trữ để đảm bảo dữ liệu ít nhất lưu trữ ở hai nơi đề phòng ổ đĩa cứng của máy tính bị hỏng.

c) Mỗi cơ quan, đơn vị, UBND các xã, thị trấn phải bố trí ngân sách, trang bị thiết bị lưu trữ ngoài (ổ cứng di động, USB, đĩa CD, DVD…) nhằm lưu trữ dữ liệu an toàn và bảo mật.

3. Định kỳ sao lưu

Tùy vào mức độ qui định thời hạn mỗi loại thông tin, dữ liệu cần sao lưu.

a) Đối với dữ liệu hệ thống: Sao lưu định kỳ: 03 tháng/lần;

b) Đối với các hệ thống thông tin: Sao lưu thường xuyên;

c) Đối với các dữ liệu khác: Sao lưu khi có thay đổi thông tin.

Điều 8. Giải quyết và khắc phục sự cố về an toàn, an ninh thông tin

1. Đối với CBCCVC

a) Thông báo kịp thời cho cán bộ phụ trách CNTT của cơ quan, đơn vị khi phát hiện các sự cố gây mất AT-ANTT trong hệ thống mạng.

b) Trường hợp xảy ra sự cố nghiêm trọng không khắc phục được phải kịp thời báo cáo cho cơ quan chuyên môn, cán bộ phụ trách CNTT của Văn phòng HĐND và UBND huyện để có giải pháp xử lý kịp thời.

c) Xử lý khẩn cấp: Khi phát hiện hệ thống bị tấn công, thông qua các dấu hiệu khác thường như: Hệ thống máy tính hoạt động chậm khác thường, nội dung bị thay đổi,… cần thực hiện các bước sau:

- Ngắt kết nối máy vi tính ra khỏi mạng LAN, Internet.

- Sao chép toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ ngoài (USB, ổ cứng di động,…).

- Khôi phục hệ thống bằng cách chuyển dữ liệu backup (sao lưu) mới nhất để hệ thống hoạt động ổn định.

2. Đối với cán bộ phụ trách CNTT

a) Quản lý việc di chuyển các trang thiết bị CNTT (máy chủ, máy trạm, thiết bị ngoại vi...) của cơ quan, đơn vị.

b) Hướng dẫn người dùng các biện pháp kỹ thuật giải quyết và khắc phục sự cố; trong trường hợp sự cố xảy ra ngoài khả năng giải quyết, kịp thời báo cáo với lãnh đạo cơ quan, đơn vị; đồng thời phối hợp với cơ quan chuyên môn, cán bộ phụ trách CNTT của huyện để cùng phối hợp khắc phục.

3. Đối với Văn phòng HĐND và UBND huyện

- Chỉ đạo cán bộ chuyên trách về CNTT, theo dõi, tổng hợp, nắm tình hình, tham mưu các văn bản chỉ đạo về AT-ANTT của huyện.

- Chủ trì, phối hợp với các cơ quan, đơn vị liên quan xử lý các sự cố, đảm bảo AT-ANTT trong các cơ quan QLNN, đơn vị sự nghiệp và UBND các xã, thị trấn của huyện.

- Tham mưu cho Chủ tịch UBND huyện các phương án xử lý đảm bảo AT-ANTT trên địa bàn huyện.

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

Điều 9. Trách nhiệm của Chủ tịch UBND huyện

1. Phân công cán bộ phụ trách CNTT đảm bảo, an toàn thông tin trước khi tiến hành các hoạt động quản lý, vận hành hệ thống thông tin.

2. Quan tâm đầu tư các thiết bị phần cứng, phần mềm liên quan đến công tác đảm bảo AT-ANTT.

3. Khi có sự cố hoặc nguy cơ mất, AT-ANTT kịp thời chỉ đạo các Phòng chức năng và cán bộ phụ trách CNTT phối hợp chặt chẽ với các cơ quan, đơn vị phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm AT-ANTT.

4. Chỉ đạo các cơ quan, đơn vị, UBND các xã, thị trấn tăng cường công tác đảm bảo AT-ANTT trong hoạt động ứng dụng CNTT và quan tâm đầu tư các thiết bị AT-ANTT, khuyến khích các đơn vị mua các phần mềm diệt virus có bản quyền cho các máy tính ở cơ quan, đơn vị.

Điều 10. Trách nhiệm của Văn phòng HĐND và UBND huyện

1. Tham mưu cho UBND huyện về công tác đảm bảo AT-ANTT và chịu trách nhiệm trước UBND huyện trong việc đảm bảo AT-ANTT cho các hệ thống thông tin của các cơ quan, đơn vị thuộc UBND huyện và UBND các xã, thị trấn.

2. Hàng năm xây dựng kế hoạch, tổng hợp kinh phí để triển khai công tác AT-ANTT trong hoạt động ứng dụng CNTT của UBND huyện.

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 AT-ANTT.

4. Tham mưu cho UBND huyện triển khai các chương trình đào tạo, bồi dưỡng, hội nghị tuyên truyền AT-ANTT trên địa bàn huyện.

5. Thường xuyên khuyến cáo về các sản phẩm CNTT mới có chất lượng và nguồn gốc đến các cơ quan đơn vị để làm cơ sở khi mua sắm sửa chữa; hướng dẫn cụ thể về nghiệp vụ quản lý vận hành, kỹ thuật đảm bảo AT-ANTT; đồng thời, hỗ trợ các cơ quan, đơn vị giải quyết sự cố khi có yêu cầu.

6. Thông báo cho các cơ quan, đơn vị biết để có biện pháp phòng ngừa, ngăn chặn các nguy cơ mất AT-ANTT do virus, phần mềm gián điệp,... gây ra.

Điều 11: Trách nhiệm của Công an huyện

1. Chủ trì, phối hợp với Văn phòng HĐND và UBND huyện và các cơ quan liên quan thực hiện quản lý, kiểm soát, phòng ngừa, đấu tranh, ngăn chặn các loại tội phạm lợi dụng hệ thống thông tin xâm hại đến an ninh chính trị, trật tự an toàn xã hội.

2. Định kỳ thông báo cho các cơ quan về phương thức, thủ đoạn mới của các loại tội phạm xâm hại đến AT-ANTT để có biện pháp phòng ngừa, đấu tranh.

3. Điều tra làm rõ các trường hợp vi phạm AT-ANTT và xử lý đúng quy định của pháp luật.

4. Hàng năm xây dựng kế hoạch bảo vệ an toàn các công trình quan trọng về an ninh quốc gia trên lĩnh vực CNTT trên địa bàn huyện.

Điều 12: Trách nhiệm của các cơ quan, đơn vị thuộc UBND huyện và UBND các xã, thị trấn

1. Tuyên truyền, nâng cao nhận thức cho CBCCVC về các nguy cơ mất AT-ANTT; tổ chức triển khai thực hiện các quy định tại Quyết định này và chịu trách nhiệm trước Chủ tịch UBND huyện trong công tác đảm bảo AT-ANTT của cơ quan, đơn vị mình.

2. Xây dựng quy trình AT-ANTT 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 như: Xây dựng quy chế đảm bảo AT-ANTT nội bộ, lập kế hoạch, xây dựng hệ thống, quản lý và vận hành hệ thống, kiểm tra đánh giá hoạt động của hệ thống, bảo trì và nâng cấp hệ thống bảo vệ an toàn, an ninh cho hệ thống thông tin.

3. Khi có sự cố hoặc nguy cơ mất an toàn thông tin phải kịp thời chỉ đạo khắc phục ngay và thông báo bằng văn bản cho Văn phòng HĐND và UBND huyện biết. Trường hợp không khắc phục được thì phối hợp với Văn phòng HĐND và UBND huyện để được hướng dẫn, hỗ trợ và tạo điều kiện thuận lợi cho cơ quan chức năng tham gia khắc phục sự cố.

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. Khi sửa chữa, nâng cấp, mua sắm các thiết bị ứng dụng CNTT cần tham khảo ý kiến chuyên môn của Văn phòng HĐND và UBND huyện về chất lượng, nguồn gốc, tính năng kỹ thuật trước khi thực hiện.

6. Tạo điều kiện thuận lợi cho cán bộ thuộc thẩm quyền quản lý của mình được tham gia các lớp tập huấn, tuyên truyền, hội nghị, hội thảo chuyên đề về an toàn thông tin do các cấp tổ chức.

7. Báo cáo tình hình và kết quả thực hiện công tác đảm bảo AT-ANTT tại cơ quan, đơn vị và gửi về Văn phòng HĐND và UBND huyện trước ngày 05 tháng 12 hàng năm.

Điều 13. Trách nhiệm của Cán bộ phụ trách CNTT

1. Xây dựng kế hoạch ứng dụng CNTT hàng năm của cơ quan, đơn vị.

2. Kịp thời tham mưu cho cơ quan, đơn vị những quy định, hướng dẫn có liên quan đến công tác đảm bảo AT-ANTT.

3. Đảm bảo AT-ANTT đối với các máy tính, hệ thống mạng của cơ quan, đơn vị trên địa bàn huyện.

4. Quản lý việc di chuyển các trang thiết bị CNTT như: máy chủ, máy trạm, thiết bị ngoại vi, hệ thống mạng..., thực hiện báo cáo kịp thời về tình trạng hoạt động toàn hệ thống mạng, đề xuất hướng giải quyết khi có sự cố.

5. Thực hiện cấp phát, thu hồi, cập nhật và quản lý tất cả các tài khoản truy cập vào hệ thống thông tin của huyện; hướng dẫn người dùng thay đổi mật khẩu cá nhân theo quy định.

6. Vận hành an toàn hệ thống thông tin của cơ quan, đơn vị, triển khai các biện pháp đảm bảo AT-ANTT cho tất cả cán bộ, công chức, viên chức trong đơn vị mình.

7. Quản lý, theo dõi các hoạt động thường xuyên và định kỳ như vận hành, sửa chữa hệ thống máy chủ, máy trạm, các thiết bị khác… Xử lý các yêu cầu về thay đổi tài khoản sử dụng mạng của các cơ quan QLNN, đơn vị sự nghiệp, UBND các xã, thị trấn trong huyện.

Điều 14. Đối với cán bộ, công chức, viên chức và người lao động

1. Các máy tính khi không sử dụng trong thời gian dài (quá 1 giờ làm việc) cần tắt máy, để tránh bị các hacker lợi dụng, sử dụng chức năng điều khiển từ xa tấn công vào hệ thống thông tin của cơ quan, đơn vị.

2. CBCCVC tự quản lý các thiết bị CNTT được giao sử dụng; không tự ý thay đổi và tháo lắp các thiết bị trên máy tính khi chưa có sự đồng ý của cán bộ phụ trách CNTT; không tự ý liên hệ với cá nhân bên ngoài vào can thiệp các thiết bị và mạng máy tính.

3. Sử dụng chức năng mã hóa đảm bảo các dữ liệu nhạy cảm như tài khoản, mật khẩu, các tập tin văn bản,... trước khi truyền trên môi trường mạng. Các tập tin gửi đính kèm bởi thư điện tử hoặc được tải xuống từ Internet hay các thiết bị lưu trữ gắn vào hệ thống cần được kiểm tra để phòng chống lây nhiễm virus hoặc phần mềm gián điệp làm mất thông tin.

4. Không được truy cập hoặc tải thông tin từ các Website độc hại, không được cài đặt các chương trình không rõ nguồn gốc…

5. Không dùng hòm thư công vụ của cá nhân và của cơ quan, đơn vị vào mục đích cá nhân như đăng ký tài khoản mạng xã hội, đăng ký mua sắm qua mạng...

6. Nghiêm chỉnh chấp hành các quy định nội bộ về AT-ANTT của cơ quan và các quy định khác của pháp luật; nâng cao ý thức cảnh giác và trách nhiệm, đảm bảo AT-ANTT tại cơ quan.

7. Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin và các vụ lộ, lọt bí mật nhà nước trong hoạt động ứng dụng công nghệ thông tin của cơ quan phải báo cáo kịp thời cho bộ phận quản lý an toàn thông tin để kịp thời ngăn chặn, xử lý.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 15. Cán bộ phụ trách CNTT huyện

1. Trực tiếp tham mưu xử lý, khắc phục sự cố, hướng dẫn khắc phục sự cố về AT-ANTT của huyện.

2. Thường xuyên hướng dẫn CBCCVC khai thác và sử dụng tài nguyên CNTT và đảm bảo AT-ANTT.

Điều 16. Văn phòng HĐND và UBND huyện

1. Chủ trì phối hợp với các cơ quan liên quan đôn đốc, hướng dẫn việc thực hiện nghiêm túc Quy định này và báo cáo UBND huyện về AT-ANTT theo quy định.

2. Tổng hợp các vướng mắc, đề nghị bổ sung, chỉnh sửa quy định; tham mưu đề xuất đầu tư kinh phí mua các phần mềm, thiết bị và hạ tầng kỹ thuật để đảm bảo AT-ANTT cho huyện.

Điều 17. Khen thưởng, xử lý vi phạm

Các phòng chuyên môn, đơn vị trực thuộc; cán bộ, công chức, viên chức và người lao động thực hiện tốt Quy chế này đem lại hiệu quả thiết thực sẽ được xem xét đánh giá bổ sung vào thang điểm xét thi đua cuối năm.

Các cơ quan chuyên môn, đơn vị trực thuộc; cán bộ, công chức, viên chức và người lao động 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.

Điều 18. Điều khoản thi hành

Các cơ quan chuyên môn, đơn vị trực thuộc tổ chức triển khai thực hiện nghiêm túc Quy chế này. Trong quá trình thực hiện, nếu có khó khăn, vướng mắc, phát sinh cần sửa đổi, bổ sung, đề nghị các phòng chuyên môn, đơn vị trực thuộc kịp thời báo cáo về Phòng Công nghệ thông tin để tổng hợp trình UBND huyện xem xét, giải quyết./.

KT.CHỦ TỊCH
PHÓ CHỦ TỊCH

Đã ký

Nguyễn Thanh Lam