ỦY BAN NHÂN DÂN HUYỆN YÊN THẾ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 03/2015/QĐ-UBND	*Yên Thế, ngày 02 tháng 6 năm 2015*

QUYẾT ĐỊNH
Ban hành Quy định 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 Yên Thế, tỉnh Bắc Giang

ỦY BAN NHÂN DÂN HUYỆN YÊN THẾ

Căn cứ Luật Tổ chức HĐND và UBND ngày 26 tháng 11 năm 2003;

Căn cứ Luật Ban hành văn bản quy phạm pháp luật của HĐND, UBND ngày 14 tháng 12 năm 2004;

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

Căn cứ Pháp lệnh bảo vệ bí mật nhà nước ngày 28 tháng 12 năm 2000;

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

Căn cứ Quyết định số 176/2012/QĐ-UBND ngày 18 tháng 6 năm 2012 của UBND tỉnh Bắc Giang về việc Ban hành quy định đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước tỉnh Bắc Giang;

Theo đề nghị của Phòng Văn hóa và Thông tin huyện tại Tờ trình số 72/VH&TT-CNTT ngày 06/5/2015,

QUYẾT ĐỊNH

Điều 1. Ban hành kèm theo Quyết định này Quy định 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 Yên Thế, tỉnh Bắc Giang.

Điều 2. Quyết định này có hiệu lực sau 7 ngày, kể từ ngày ký.

Điều 3. Thủ trưởng các cơ quan, đơn vị thuộc Huyện ủy, Ủy ban nhân dân huyện, Chủ tịch UBND các xã, thị trấn và các cơ quan, đơn vị, cá nhân liên quan căn cứ Quyết định thi hành./.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Vũ Trí Hải

ỦY BAN NHÂN DÂN
HUYỆN YÊN THẾ

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

QUY ĐỊNH
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 Yên Thế

(Ban hành kèm theo Quyết định số 03/2015/QĐ-UBND ngày 02 tháng 6 năm 2015 của Ủy ban nhân dân huyện)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh: Quy định 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, đơn vị sự nghiệp, UBND các xã, thị trấn của huyện Yên Thế (sau đây gọi tắt là cơ quan, đơn vị).

2. Đối tượng áp dụng: Quy định này được áp dụng đối với các các tổ chức, cá nhân liên quan đến an toàn, an ninh thông tin trong các cơ quan nhà nước, đơn vị sự nghiệp, cán bộ công chức, viên chức và người lao động tham gia vào việc vận hành, khai thác và sử dụng hệ thống thông tin của các cơ quan trên địa bàn huyện.

Điều 2. Giải thích từ ngữ

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

1. Ứng dụng CNTT là việc sử dụng CNTT vào các hoạt động thuộc lĩnh vực kinh tế - xã hội, quốc phòng, an ninh và các hoạt động khác nhằm nâng cao năng suất, chất lượng, hiệu quả của các hoạt động này.

2. An toàn thông tin là sự bảo vệ thông tin và hệ thống thông tin tránh bị truy cập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

3. 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.

4. Hệ thống thông tin là tập hợp các thiết bị viễn thông, CNTT bao gồm phần cứng, phần mềm và cơ sở dữ liệu phục vụ cho hoạt động lưu trữ, xử lý, truyền đưa, chia sẻ, trao đổi, cung cấp và sử dụng thông tin.

Điều 3. Mục đích, nguyên tắc đảm bảo an toàn thông tin

1. Việc áp dụng Quy định này nhằm giảm thiểu được các nguy cơ gây mất an toàn thông tin, đảm bảo an ninh và bí mật 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.

Điều 4. Các hành vi bị nghiêm cấm

1. Tạo ra, cài đặt, phát tán virus máy tính, phần mềm độc hại trái pháp luật.

2. Xâm nhập, sửa đổi, xóa bỏ nội dung thông tin của cơ quan, cá nhân khác khi chưa được sự cho phép.

3. Cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin.

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

5. 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 5. Cán bộ phụ trách CNTT

1. Cán bộ phụ trách CNTT là người có phẩm chất đạo đức và phẩm chất chính trị tốt, được đào tạo cơ bản về kiến thức CNTT (có chứng chỉ về an toàn an ninh thông tin).

2. Đối với cán bộ phụ trách CNTT khối Huyện ủy, UBND huyện tối thiểu phải có trình độ cao đẳng CNTT trở lên, có chứng chỉ về an toàn, an ninh thông tin. Đối với các cơ quan, đơn vị; các xã, thị trấn cán bộ được phân công phụ trách CNTT tối thiểu phải có chứng chỉ B về CNTT trở lên và thường xuyên được đào tạo, tập huấn về kiến thức CNTT.

Chương II
NỘI DUNG ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 6. Quản lý cán bộ, công chức, viên chức và người lao động

1. Các cơ quan, đơn vị phải xây dựng các yêu cầu, trách nhiệm đảm bảo an toàn thông tin đối với từng vị trí công việc. 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, đơn vị.

2. 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, thư mục lưu trữ, thư điện tử, máy vi tính, ...) đối với các cá nhân nghỉ việc, chuyển công tác.

Điều 7. Quản lý hệ thống thông tin

1. Máy chủ

a) Cơ sở dữ liệu các phần mềm dùng chung được lưu trữ trên máy chủ đặt tại Trung tâm CNTT và Truyền thông thuộc Sở Thông tin và Truyền thông.

b) Khuyến khích các cơ quan sử dụng máy chủ chạy chương trình phần mềm chuyên ngành chuyển dữ liệu về Trung tâm tích hợp của Sở Thông tin và Truyền thông quản lý để đảm bảo an toàn, an ninh dữ liệu.

2. Các thiết bị CNTT, hệ thống mạng

a) Máy tính và thiết bị mạng phải được lắp đặt gọn gàng, thường xuyên được vệ sinh sạch sẽ, đảm bảo an toàn, điện lưới ổn định, thiết bị lưu điện, hệ thống chống cháy nổ...

b) Khi các thiết bị thông tin bị sự cố, người trực tiếp sử dụng phải kịp thời báo cho cán bộ phụ trách CNTT của cơ quan, đơn vị. Cán bộ phụ trách CNTT phối hợp với cán bộ kế toán đơn vị xác định nguyên nhân, mức độ và biện pháp khắc phục sự cố. Nếu không xử lý được báo cáo Thủ trưởng đơn vị phương án sửa chữa, khắc phục. Trong quá trình sửa chữa, cán bộ phụ trách CNTT của các cơ quan, đơn vị phải trực tiếp giám sát và chịu trách nhiệm trước Thủ trưởng cơ quan về vấn đề an toàn, bảo mật các thông tin lưu trữ trong máy tính, không để lọt thông tin ra ngoài.

3. Phòng chống mã độc

a) Tất cả các máy tính 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 khi sao chép, mở các tập tin.

b) Các cán bộ, công chức, viên chức và người lao động 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 tính khi chưa có sự đồng ý của người có thẩm quyền theo quy định của cơ quan.

c) 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.

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

c) Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm mã độc trên máy tính (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.

3. Sao lưu dữ liệu dự phòng

a) Các dữ liệu quan trọng của cơ quan phải được định kỳ sao lưu, bao gồm: thông tin cấu hình của hệ thống mạng; phần mềm ứng dụng và cơ sở dữ liệu.

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

4. Quản lý truy cập

a) Việc quản lý truy cập vào hệ thống thông tin, mạng máy tính, thiết bị, phần mềm ứng dụng của đơn vị phải được quy định chi tiết và tổ chức thực hiện nghiêm túc, phù hợp với các quy định của pháp luật về an toàn thông tin.

b) Mỗi tài khoản truy cập các hệ thống thông tin chỉ được cấp cho một người quản lý và sử dụng.

c) Mỗi cán bộ, công chức, viên chức và người lao động 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.

d) 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 nếu liên tục đăng nhập sai vượt quá số lần quy định.

e) Tất cả máy tính phải được đặt mật khẩu truy cập và thiết lập chế độ tự động bảo vệ màn hình sau 10 phút không sử dụng.

g) Khi thiết lập mạng không dây trong nội bộ đơn vị, phải đặt mật khẩu truy cập vào mạng không dây và chỉ cho phép truy cập Internet.

f) 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.

Chương III
TỔ CHỨC THỰC HIỆN

Điều 8. Trách nhiệm của cán bộ, công chức, viên chức và người lao động trong các cơ quan

1. Trách nhiệm của cán bộ phụ trách CNTT

a) Trực tiếp chịu trách nhiệm đảm bảo an toàn, bảo mật thông tin của cơ quan, 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, bảo mật thông tin;

c) Thực hiện việc kiểm tra, giám sát, báo cáo thủ trưởng cơ quan các hình thức, mức độ nghiêm trọng về mất an toàn thông tin;

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

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

b) Mỗi cán bộ, công chức, viên chức và người lao động phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao quản lý, sử dụng; không tự ý thay đổi, tháo lắp các thiết bị trên máy tính; không được 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 cán bộ phụ trách CNTT của cơ quan để kịp thời có biện pháp ngăn chặn và xử lý;

d) Tham gia các chương trình đào tạo, hội nghị về an toàn an ninh thông tin do huyện hoặc Sở Thông tin và Truyền thông tổ chức.

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

1. Thủ trưởng cơ quan, đơn vị

a) Có trách nhiệm tổ chức thực hiện quy định này và chịu trách nhiệm trước Ủy ban nhân dân huyện trong công tác đảm bảo an toàn, bảo mật thông tin của cơ quan, đơn vị mình.

b) Phân công cán bộ phụ trách CNTT, 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 về an toàn thông tin.

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

d) 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 kịp thời, nhanh chóng và có hiệu quả sự cố xảy ra.

2. Trách nhiệm của Phòng Văn hóa và Thông tin (cơ quan Thường trực BCĐ CNTT của huyện)

a) Tham mưu giúp Ủy ban nhân dân huyện quản lý nhà nước về công tác đảm bảo an toàn, an ninh, bảo mật thông tin trên địa bàn huyện.

b) Hằng 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 của huyện.

c) Chủ trì, phối hợp với các cơ quan, đơn vị liên quan tổ chức kiểm tra theo định kỳ hoặc đột xuất; kịp thời phát hiện và đề xuất phương án 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, bảo mật thông tin trên địa bàn huyện.

d) Hằng năm xây dựng và phối hợp với Trung tâm CNTT&TT thuộc Sở Thông tin và Truyền thông triển khai các chương trình đào tạo chuyên sâu về an toàn, an ninh thông tin cho cán bộ phụ trách CNTT của các cơ quan, đơn vị.

e) 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.

g) Tổng hợp và báo cáo tình hình an toàn, an ninh thông tin theo định kỳ về Sở Thông tin và Truyền thông, Ủy ban nhân dân huyện và các cơ quan, đơn vị có liên quan.

3. Trách nhiệm của Công an huyện

a) Chủ trì, phối hợp với 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, bảo mật thông tin trong cơ quan nhà nước.

b) 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, bảo mật thông tin.

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

d) 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.

Điều 10. Điều khoản thi hành

1. Giao Phòng Văn hóa và Thông tin chủ trì, phối hợp với các cơ quan liên quan đôn đốc, hướng dẫn triển khai thực hiện nghiêm túc Quy định này.

2. Các cơ quan, đơn vị, cá nhân có hành vi vi phạm Quy đinh tùy theo tính chất, mức độ vi phạm mà bị xử lý theo Quy định của Pháp luật hiện hành.

3. Trong quá trình thực hiện nếu có những vấn đề cần sửa đổi, bổ sung, đề nghị các đơn vị phản ảnh về UBND huyện (thông qua Phòng Văn hóa và Thông tin) để tổng hợp báo cáo UBND huyện xem xét, quyết định.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Vũ Trí Hải