UBND TỈNH BÌNH ĐỊNH **SỞ XÂY DỰNG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 72 /QĐ-SXD	*Bình Định, ngày 02 tháng 6 năm 2014*

QUYẾT ĐỊNH

Về việc ban hành Quy chế nội bộ đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Sở Xây dựng Bình Định

GIÁM ĐỐC SỞ XÂY DỰNG

Căn cứ Luật Công nghệ thông tin số 67/2006/QH11 ngày 29/6/2006;

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

Căn cứ Chỉ thị số 897/CT-TTg, ngày 10/6/2011 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/QĐ-UBND ngày 12/7/2012 của UBND tỉnh Bình Định 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 quản lý hành chính nhà nước tỉnh Bình Định;

Căn cứ Quyết định 707/QĐ-UBND ngày 30/9/2009 của UBND tỉnh về việc ban hành Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Xây dựng;

Theo đề nghị của Chánh Văn phòng Sở Xây dựng,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này "Quy chế nội bộ đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Sở Xây dựng Bình Định".

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

Điều 3. Chánh Văn phòng Sở, Trưởng các phòng chuyên môn, đơn vị trực thuộc và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Sở Thông tin và Truyền thông;
- Lãnh đạo Sở;
- Lưu: VT, VP .

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ XÂY DỰNG
TỈNH BÌNH ĐỊNH

Đào Quý Tiêu

UBND TỈNH BÌNH ĐỊNH
SỞ XÂY DỰNG

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

Số : /QĐ-SXD

Bình Định, ngày tháng năm 2014

QUY CHẾ NỘI BỘ
Đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Sở Xây dựng Bình Định

(Ban hành kèm theo Quyết định số 72/QĐ-SXD, ngày 02/ 6/2014 của Giám đốc Sở Xây dựng)

Chương I
NHỮNG QUY ĐỊNH CHUNG

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

1. Quy chế này quy định về công tác bảo đảm an toàn, an ninh thông tin trong lĩnh vực ứng dụng công nghệ thông tin phục vụ cho công tác điều hành và quản lý hành chính nhà nước của Sở Xây dựng Bình Định.

2. Quy chế này được áp dụng đối với cán bộ, công chức, viên chức và hợp đồng lao động của Khối Văn phòng Sở và các đơn vị trực thuộc Sở trong việc vận hành, khai thác và sử dụng hệ thống thông tin cơ quan.

Điều 2. Mục tiêu và phương hướng công tác đảm bảo an toàn, an ninh thông tin

1. Giảm thiểu được các nguy cơ gây sự cố mất an toàn thông tin và đảm bảo an ninh thông tin trong quá trình tham gia hoạt động trên môi trường mạng của cán bộ công 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 sử dụng tốt, có hiệu quả việc ứng dụng công nghệ thông tin trong công tác chuyên môn của Sở Xây dựng.

Điều 3. Giải thích từ ngữ

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

1. An toàn, an ninh 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 sự cố xảy ra trong khi sử dụng hoặc do người sử dụng vô ý hoặc cố ý gây ra. Việc bảo vệ thông tin, dữ liệu và tài khoản của người sử dụng trong hệ thống thông tin nhằm bảo đảm cho các hệ thống thực hiện đúng chức năng, phục vụ những mục đích, tính sẵn sàng cao với yêu cầu chính xác và tin cậy. An toàn, an ninh thông tin bao hàm các nội dung bảo vệ và bảo mật thông tin, an toàn dữ liệu của máy tính và an toàn, an ninh mạng.

2. Hệ thống an ninh mạng: Là lập hợp các thiết bị tường lửa; thiết bị kiểm soát, phát hiện truy cập bất hợp pháp; phần mềm quản trị, theo dõi,

ghi nhật ký trạng thái an ninh mạng và các trang thiết bị khác có chức năng đảm bảo an toàn hoại động của mạng, tất cả cũng hoạt động đồng bộ theo một chính sách an ninh mạng nhất quán nhằm kiểm soát chặt chẽ tất cả các hoạt động trên mạng.

3. Virus máy tính: là một chương trình hay một đoạn mã có khả năng tự sao chép chính nó từ đối tượng lây nhiễm này sang đối tượng khác (đối tượng là các máy tính, tập tin văn bản).

4. Phần mềm độc hại (mã độc): là các phần mềm có tính năng gây hại như virus, phần mềm do thám (spyware), phần mềm quảng cáo (adware), phần mềm Crack có cài mã độc hoặc các dạng tương tự khác.

5. Frirewall: Là tập hợp các thành phần hoặc một hệ thống các trang thiết bị, phần mềm được đặt giữa hai mạng, nhằm kiểm soát tất cả các kết nối từ bên trong ra bên ngoại mạng và ngược lại.

6. Người sử dụng: Cán bộ, công chức, viên chức và hợp đồng lao động của Sở Xây dựng và các đơn vị trực thuộc.

Chương II

QUY CHẾ NỘI BỘ BẢO ĐẢM AN TOÀN, AN NINH THÔNG TIN

Điều 4. Phân loại và quản lý mức độ ưu tiên đối với các nguồn tài nguyên của hệ thống thông tin

1. Đối với phần mềm

Các phần mềm có bản quyền (đã được cơ quan, đơn vị mua hoặc cung cấp nhằm phục vụ cho hoạt động đảm bảo an toàn cho hệ thống thông tin; các phần mềm ứng dụng như: Phần mềm kế toán, văn thư. lưu trữ, văn phòng, điện tử, tính dự toán... phải đảm bảo tính chính xác của thông tin, không gây ra sự cố mất dữ liệu, đảm bảo hệ thống phần mềm luôn hoạt động liên tục.

2. Đối với dữ liệu

Người sử dụng có trách nhiệm tự quản lý dữ liệu lưu trữ trên máy tính phục vụ công tác chuyên môn của mình, định kỳ ít nhất 6 tháng mỗi lần, phải tiến hành lưu trữ, sao chép dữ liệu trong máy tính ra bộ nhớ ngoài như: ổ cứng bên ngoài máy, đĩa CD, USB... các thiết bị lưu trữ thông tin này phải được bảo quản ở nơi an toàn và bảo mật.

3. Đối với trang thiết bị

- Tất cả máy tính cơ quan cần được trang bị phần mềm diệt virus có bản quyền, ngoại trừ những máy tính có cấu hình thấp không thể cài đặt được, cần phải lựa chọn phần mềm diệt virus miễn phí phù hợp với cấu hình máy tính, nhưng phải đảm bảo độ tin cậy cao trên những máy tính đó để đảm bảo an toàn an ninh thông tin cho hệ thống mạng máy tính cơ quan.

- Các thiết bị gắn ngoài như USB, thẻ nhớ, máy tính xách tay, máy tính bảng, điện thoại di động của cơ quan trang bị hoặc tự có khi cắm vào máy tính hoặc mạng LAN, Internet Wifi của cơ quan cần phải sạch không, có virus hoặc các phần mềm độc hại khác.

- Người sử dụng có trách nhiệm quản lý, bảo quản thiết bị được giao sử dụng; không tự ý thay đổi cấu hình hoặc tháo lắp, sửa chữa các thiết bị trên máy tính khi chưa có sự đồng ý của lãnh đạo cơ quan, đơn vị.

Điều 5. Quản lý, vận hành Hệ thống bảo vệ an toàn, an ninh thông tin.

1. Hệ thống mạng nội bộ.

- Hệ thống mạng nội bộ (LAN) được thiết lập và quản lý theo nhóm (Group) từng phòng, ban và cấp địa chỉ mạng (IP) cố định cho từng máy tính cá nhân của phòng, ban cơ quan trong mạng LAN theo danh sách địa chỉ IP cố định đã ban hành.

- Hệ thống mạng không dây của Sở được kết nối với mạng nội bộ thông qua các điểm truy nhập (Aeeess Point) theo chuẩn N, với tốc độ 100Mb/giây (Mbps) và thiết lập các tham số bảo mật truy cập theo chuẩn bảo mật mạng không dây an toàn nhất hiện nay là WPA2 và định kỳ 3 tháng thay đổi mật khẩu nhằm tăng cường công tác bảo mật.

- Hệ thống máy chủ, router, switch, thiết bị FTTH được đặt cố định; nguồn điện cung cấp cho hệ thống này phải ổn định; có điều hòa nhiệt độ để đảm bảo về nhiệt độ và độ ẩm phù hợp với yêu cầu tiêu chuẩn kỹ thuật phòng máy.

2. Tổ chức quản lý tài khoản

- Cán bộ chuyên trách CNTT của Sở có trách nhiệm tạo, lập và cung cấp tài khoản truy nhập hệ thống mạng nội bộ (IP), hệ thống email công vụ, hệ thống thông tin tác nghiệp, hệ thống văn phòng điện tử. . , cho người sử dụng.

- Đối với người sử dụng tiếp nhận mới hoặc chuyển công tác, nghỉ hưu, nghỉ việc; Cán bộ chuyên trách CNTT căn cứ quyết định của cơ quan tạo mới hoặc hủy bỏ các tài khoản liên quan của các cá nhân đó.

3. Quản lý đăng nhập hệ thống

- Người sử dụng đã được cấp tài khoản trên Trang thông tin tác nghiệp, hộp thư điện tử công vụ, văn phòng điện tử tại Sở Xây dựng cần đổi mật khẩu ban đầu có tính bảo mật cao (ví dụ: 12!@bnm) ngày làm truy cập đầu tiên đối với các tài khoản này; Định kỳ 03 tháng phải thay đổi mật khẩu và không dùng một mật khẩu trong nhiều tại khoản.

- Khi đăng nhập vào hệ thống và máy tính được trang bị phải có trách nhiệm bảo vệ và bảo mật tài khoản, dữ liệu máy tính của mình như: kế toán, văn thư, lưu trữ, văn phòng điện tử, hộp thư công vụ, ..; không tự ý xâm nhập các tài khoản khác; đồng thời không cung cấp thông tin tài khoản của mình cho các cá nhân không có liên quan.

4. Đối với máy tính, thiết bị tháo lắp (USB, máy tính xách tay..)

- Người sử dụng được giao sử dụng máy tính phải đặt mật khẩu truy cập vào máy tính của mình và cài đặt cơ chế tự động thoát cho máy tính khi không sử dụng máy tính trong thời gian dài.

- Khi mở các tập tin đính kèm theo thư điện tử hoặc được tải xuống

từ Internet hay các thiết bị lưu trữ (USB) gắn vào hệ thống, nếu biết rõ người gửi thư thì phải lựa tập tin vào máy tính rồi quét virus trước khi mở; không tải các thư điện tử có tập tin đính kèm không rõ nguồn gốc vì rất có thể có virus, phần mềm gián điệp được đính kèm theo thư điện tử được kích hoạt và lây lan vào máy tính thông qua thao tác đó gây mất dữ liệu thông tin.

- Khi truyền dữ liệu giữa USB và máy tính, không trực tiếp truy nhập ngay vào USB (vì có thể rất nhiều virus được kích hoại và lây lan vào máy tính thông qua thao tác đó) mà phải quét virus đối với USB bằng phần mềm diệt virus, sau đó mới được truy cập bình thường.

5. Truyền tải, lưu trữ, sao chép thông tin

- Để đảm bảo an toàn an ninh thông tin trong việc truyền tải, lưu trữ, sao chép thông tin, người sử dụng cần hạn chế việc chia sẻ thông tin, dữ liệu trên máy tính qua tính năng share full của window và cần đổi mật khẩu cho máy tính cá nhân định kỳ 3 tháng. Phải bảo mật, quản lý, sử dụng các tài khoản Hệ thống thư điện tử công vụ và trang thông tin tác nghiệp... của Sở để truy nhập, thu thập, chia sẻ dữ liệu, truyền tải thông tin, tài liệu... trên ra môi trường mạng,

- Không được lưu trữ dữ liệu và sao chép thông tin trên phân vùng đĩa cứng cài đặt hệ điều hành (ổ cứng C), việc lưu trữ dữ liệu và sao chép thông tin chỉ thực hiện trên đĩa cứng D, H hoặc trên USB, giúp cho việc phục hồi mọi dữ liệu trên địa C được dễ dàng khi có sự cố máy tính xảy ra.

6. Chống mã độc, virus

- Người sử dụng cần cài đặt phần mềm chống virus (do cơ quan mua hoặc tự mua) lên các máy tính cá nhân, máy tính xách tay, các thiết bị di động,.. trước khi đăng nhập vào hệ thống mạng internet của cơ quan để phát hiện, loại trừ những đoạn mã độc hại (Virus, trojan, worms..) được truyền tải bởi: thư điện tử, tập tin đính kèm từ Internet, thiết bị lưu trữ tháo lắp nhằm khai thác lỗ hổng của hệ thống thông tin thường xuyên cập nhật các phiên bản (Version) mới, các bản vá lỗi của các phần mềm hệ thống (đối với phần mềm có bản quyền), phần mềm chống virus, phần mềm ứng, dụng,., để bảo đảm chương trình quét virus luôn được cập nhật mới nhất.

Điều 6. Giải quyết và khắc phục mọi sự cố an ninh thông tin

1. Đối với người sử dụng

- Thông tin báo cáo kịp thời cho cán bộ quản trị mạng và Lãnh đạo Sở khi phải hiện các sự cố gây mất an toàn an ninh thông tin nghiêm trọng không khắc phục được,

- Xử lý khẩn cấp: Khi bị 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 cần thay đổi,... cần thực hiện các bước sau:

+ Ngắt kết nốii máy tính ra khỏi mạng LAN, Imernet.

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

+ Khôi phục hệ thống bán, cách chuyển dữ liệu backup (sao lưu) mới

nhất để hệ thống hoạt động ổn định.

2. Đối với cán bộ chuyên trách CNTT

Hướng dẫn người sử dụng 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 Sở, đồng thời phối hợp với cơ quan chuyên môn để khắc phục.

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

Điều 7. Trách nhiệm của Lãnh đạo Sở

1. Lãnh đạo Sở có trách nhiệm toàn diện trước UBND tỉnh trong công tác bảo vệ an toàn hệ thống thông tin của đơn vị.

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

3. Phân bổ kinh phí để trang bị các thiết bị phần cứng, phần mềm liên quan đến công tác đảm bảo an toàn thông tin, đầu tư các thiết bị tường lửa, các chương trình chống spam, virus, phần mềm gián điệp có bản quyền trên các máy vi tính của CBCC cơ quan.

4. 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.

5. Quan tâm đào tạo, bồi dưỡng nguồn nhân lực có kiến thức, trình độ về công nghệ thông tin. Trang bị đầy đủ các kiểu 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.

6. Khi có sự cố hoặc nguy cơ mất an toàn thông tin, kịp thời cử cán bộ phối hợp chặt chẽ với cơ quan chuyên môn trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm 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.

7. Chỉ đạo các đơn vị trực thuộc tăng cường công tác an toàn, an ninh thông tin trong hoạt động ứng dụng CNTT và quan tâm đầu tư các thiết bị an toàn, an ninh thông tin ở đơn vị.

Điều 8. Trách nhiệm của cán bộ chuyên trách CNTT

1. Theo dõi, quản lý chặt chẽ việc di chuyển các trang thiết bị CNTT, hệ thống mạng trong cơ quan.

2. Thực hiện cấp phát, thu hồi, cập nhật và quản lý tất cả các tài khoản truy cập vào hệ thống thông tin của Sở; hướng dẫn người dùng thay đổi mật khẩu cá nhân theo quy định; xử lý các yêu cầu về thay đổi tài khoản sử dụng mạng của các phòng chuyên môn.

3. Tham mưu cho lãnh đạo Sở trong việc đầu tư thiết bị phần cứng, phần mềm, công tác bảo mật thông tin trên môi trường mạng; quản lý, kiểm tra và đề xuất sửa chữa, thay thế, nâng cấp phần cứng khi có yêu cầu. Các

công việc sửa chữa hàng ngày đều được ghi vào nhật ký sửa chữa của cán bộ chuyên trách CNTT sau mỗi lần sửa chữa.

4. Quản lý, vận hành các hoạt động của hệ thống mạng máy tính của Sở theo nhiệm vụ được phân công; triển khai các biện pháp bảo đảm an toàn, an ninh thông tin trong đơn vị. Kiểm tra, khắc phục sự cố kịp thời khi người sử dụng báo cáo sự cố hoặc đề nghị xem xét giải quyết khi máy tính bị sự cố.

5. Thống kê, quản lý các thiết bị lưu trữ và sao lưu dữ liệu, đồng thời lập kế hoạch nâng cấp, thay thế các thiết bị khi không còn khả năng lưu trữ; thực hiện thiết lập cơ chế sao lưu và phục hồi này chủ để thực hiện công, tác bảo trì, bảo dưỡng định kỳ, đột xuất, giảm thiểu tối đa các sự cố kỹ thuật;

6. Thực hiện việc đánh giá, báo cáo các rủi ro về mức độ nghiêm trọng có thể xảy ra do sự truy cập và sử dụng trái phép, thay đổi hoặc phá hủy thông tin và hệ thống thông tin; đề nghị hướng giải quyết khi có sự cố. Định kỳ báo cáo tổng hợp tình hình an toàn, an ninh của hệ thống của Sở cho các cơ quan liên quan theo quy định.

Điều 9. Trách nhiệm của người sử dụng

1. Nghiêm chỉnh chấp hành các quy định về an toàn thông tin của cơ quan, đơn vị liên quan đến công tác ứng dụng CNTT đã được UBND tỉnh và Sở ban hành như Quy chế quản lý, sử dụng Hệ thống thư điện tử công vụ của tỉnh: Quy định cung cấp và quản lý thông tin trên trang tin điện tử của Sở,... và 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.

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

3. Các máy lĩnh khi không sử dụng trong thời gian dài (quá 02 giờ làm việc) cần tắt máy hoặc ngừng kết nối mạng, để tránh bị các 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.

4. Không được tự ý thay đổi các tham số địa chỉ IP mạng của mạng LAN. Trường hợp cần thiết phải thay đổi tham số mạng phải báo cho cán bộ huyện trách CNTT để xử lý.

5. Không được truy cập thông tin hoặc nhấp chuột vào trang web có đường dẫn lạ không rõ về nội dung hoặc các website độc hại; không tải và cài đặt các phần mềm chưa rõ nguồn gốc. Hạn chế tải những File có dung lượng, lớn (trên 300 MB) trong giờ làm việc làm ảnh hưởng đến tốc độ đường truyền của hệ thống. 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 gây mất mát thông tin. Không dùng máy tính cơ quan trao đổi trò chuyện (chát) hoặc sử dụng facebook trao đổi với bạn bè, người thân trong giờ

hành chính, gây ảnh hưởng đến công việc chuyên môn.

6. Trong quá trình sử dụng các thiết bị CNTT, nếu có sự cố xảy ra, cán bộ, công chức, viên chức lập phiếu trình đề xuất sửa chữa, chuyển đến cán bộ chuyên trách CNTT kiểm tra xác định hư hỏng và đề xuất Lãnh đạo Sở cho sửa chữa.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 10. Khen thưởng và xử lý vi phạm

1. Các phòng chuyên môn, đơn vị trực thuộc; người sử dụng thực hiện tốt Quy chế này đem lại hiệu quả thiết thực sẽ được xem xét đánh giá trong công tác thi đua, khen thưởng; hàng năm.

2. Các phòng chuyên môn, đơn vị trực thuộc; người sử dụng có hành vi vi phạm quy chế này thì sẽ bị trừ điểm thi đua hoặc tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật trách nhiệm, xử phạt hành chính, Nếu gây thiệt hại thì phải bồi thường theo quy định.

Điều 11. Điều khoản thi hành

Chánh Văn phòng Sở, Trưởng các phòng chuyên môn, đơn vị trực thuộc Sở có trách nhiệm tổ chức thực hiện Quy chế này.

Trong quá trình thực hiện, nếu có phát sinh khó khăn, vướng mắc các phòng ban, đơn vị báo cáo lãnh đạo Sở (qua Văn phòng Sở) để kịp thời sửa đổi bổ sung cho phù hợp./.

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ XÂY DỰNG
TỈNH BÌNH ĐỊNH

Đào Quý Tiêu