UBND TỈNH BÌNH PHƯỚC **SỞ XÂY DỰNG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 584 /QĐ-SXD	*Bình Phước, ngày 28 tháng 3 năm 2017*

QUYẾT ĐỊNH

Ban hành quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng Công nghệ thông tin của Sở Xây dựng tỉnh Bình Phước

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

Căn cứ Luật ban hành văn bản quy phạm pháp luật của HĐND, UBND ngày 03/12/2004;

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

Căn cứ Luật Viễn thông ngày 23/11/2009;

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

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 90/2008/NĐ-CP ngày 13/8/2008 của Chính phủ về chống thư rác;

Căn cứ Nghị định số 77/2012/NĐ-CP ngày 05/10/2012 của Chính phủ về sửa đổi, bổ sung một số điều của Nghị định số 90/2008/NĐ-CP ngày 13/8/2008 của Chính phủ về chống thư rác;

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

Căn cứ Thông tư số 23/2011/TT-BTTTT ngày 11/8/2011 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về việc quản lý, vận hành, sử dụng và bảo đảm an toàn thông tin trên Mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước;

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

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

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 Sở Xây dựng tỉnh Bình Phước.

Điều 2. Chánh Văn phòng Sở, Trưởng các phòng ban, đơn vị trực thuộc chịu trách nhiệm thi hành Quyết định này kể từ ngày ký.

GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ XÂY DỰNG
TỈNH BÌNH PHƯỚC

Huỳnh Thanh Dũng

Nơinhận:
-Như điều 2 ;
-Lưu:VT,

UBND TỈNH BÌNH PHƯỚC
SỞ XÂY DỰNG

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

Bình Phước, ngày 28 tháng 3 năm 2017

QUY CHẾ
Bảo đảm an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của Sở Xây dựng tỉnh Bình Phước

(Ban hành kèm theo Quyết định số: 584 QĐ-SXD ngày 28 tháng 3 năm 2017 của Sở Xây dựng)

CHƯƠNG I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về nội dung, biện pháp bảo đảm an toàn, an ninh thông tin trong lĩnh vực ứng dụng công nghệ thông tin (sau đây gọi tắt là CNTT) phục vụ cho công tác điều hành và quản lý hành chính nhà nước của Sở Xây dựng tỉnh Bình Phước.

Điều 2. Đối tượng áp dụng Quy chế này được áp dụng với tất cả các phòng, ban và các đơn vị sự nghiệp thuộc Sở Xây dựng tỉnh Bình Phước.

Điều 3. Giải thích từ ngữ trong Quy chế này, các từ ngữ dưới đây được hiểu như sau:

1. *An toàn thông tin* là sự bảo vệ thông tin và hệ thống thông tin tránh bị truy nhập, 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.

2. *Hệ thống thông tin* là tập hợp thiết bị 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.

3. *Xâm phạm an toàn thông tin* là hành vi truy nhập, sử dụng, tiết lộ, làm gián đoạn, sửa đổi, làm sai lệch chức năng, phá hoại trái phép thông tin và hệ thống thông tin.

4. *Nguy cơ mất an toàn thông tin* là những nhân tố bên trong hoặc bên ngoài có khả năng ảnh hưởng tới trạng thái an toàn thông tin.

5. *Đánh giá rủi ro an toàn thông tin* là việc xác định, phân tích nguy cơ mất an toàn thông tin có thể có và dự báo mức độ, phạm vi ảnh hưởng và khả năng gây thiệt hại khi xảy ra sự cố mất an toàn thông tin.

6. *Quản lý rủi ro an toàn thông tin* là việc thực hiện đánh giá rủi ro an toàn thông tin, xác định yêu cầu bảo vệ thông tin và hệ thống thông tin và áp dụng giải pháp phòng, chống, giảm thiểu thiệt hại khi có sự cố mất an toàn thông tin.

7. *Mạng* là khái niệm chỉ mạng viễn thông cố định, di động, Internet và mạng máy tính.

8. *Phần mềm độc hại* là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hoặc toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

Điều 4. Các hành vi bị nghiêm cấm:

1. Ngăn chặn trái pháp luật việc truyền tải thông tin trên mạng; can thiệp, truy nhập, gây nguy hại, xóa, thay đổi, sửa chữa, sao chép, làm sai lệch trái phép thông tin trên mạng;

2. Cản trở trái pháp luật, gây ảnh hưởng tới sự hoạt động bình thường của hệ thống thông tin hoặc cản trở trái pháp luật, gây ảnh hưởng tới khả năng truy nhập hợp pháp của người sử dụng tới hệ thống thông tin;

3. Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của biện pháp bảo vệ an toàn thông tin cho hệ thống thông tin; lợi dụng sơ hở, điểm yếu của hệ thống thông tin, tấn công, chiếm quyền điều khiển trái phép đối với hệ thống thông tin;

4. Phát tán thư rác, tin nhắn rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo;

5. Lợi dụng mạng để truyền bá thông tin, quan điểm, thực hiện các hành vi gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, lợi ích quốc gia trên mạng; phá hại khối đại đoàn kết toàn dân; tuyên truyền chiến tranh xâm lược, khủng bố; gây hận thù, mâu thuẫn giữa các dân tộc, sắc tộc, tôn giáo và bài ngoại;

6. Lợi dụng mạng để truyền bá trái phép tài liệu, hình ảnh, âm thanh hoặc dạng thông tin khác nhằm kích động bạo lực, dâm ô, đồi trụy, tội ác, tệ nạn xã hội, mê tín dị đoan, phá hoại thuần phong, mỹ tục của dân tộc; bôi nhọ, gây thù hận, xâm hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân;

7. Các hành vi bị nghiêm cấm khác theo quy định của pháp luật.

CHƯƠNG II
NỘI DUNG BẢO ĐẢM AN TOÀN, AN NINH THÔNG TIN

Điều 5. Các biện pháp quản lý kỹ thuật cơ bản cho công tác an toàn, an ninh thông tin

1. Tổ chức mô hình mạng: Cài đặt, cấu hình, tổ chức hệ thống mạng theo mô hình Clients/Server, hạn chế sử dụng mô hình mạng ngang hàng. 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: định kỳ 3 tháng thay đổi mật khẩu nhằm tăng cường công tác bảo mật.

3. Tổ chức quản lý tài khoản: Các tài khoản và định danh người dùng trong hệ thống thông tin, bao gồm: tạo mới, kích hoạt, sửa đổi và loại bỏ các tài khoản, đồng thời tổ chức kiểm tra các tài khoản của hệ thống thông tin ít nhất 6 tháng 1 lần thông qua các công cụ của hệ thống. Hủy tài khoản, quyền truy nhập hệ thống thông tin, thu hồi lại tất cả các tài sản liên quan tới hệ thống thông tin đối với cán bộ, công chức, viên chức đã chuyển công tác, chấm dứt hợp đồng lao động.

4. Quản lý Logfile: Hệ thống thông tin cần ghi nhận các sự kiện: quá trình đăng nhập vào hệ thống, các thao tác cấu hình hệ thống. Thường xuyên kiểm tra, sao lưu (backup) các logfile theo từng tháng để lưu vết theo dõi, xác định những sự kiện đã xảy ra của hệ thống và hạn chế việc tràn logfile gây ảnh hưởng đến hoạt động của hệ thống.

5. Chống mã độc, virus: Lựa chọn, triển khai các phần mềm chống virus, 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 (Version) mới, các bản vá lỗi của các phần mềm chống virus để bảo đảm chương trình quét virus của cơ quan trên các máy chủ, máy trạm luôn được cập nhật mới nhất, thiết lập chế độ quét thường xuyên ít nhất là hằng tuần.

6. 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 phòng/đơn vị trực thuộc; 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.

7. Các biện pháp kỹ thuật bảo đảm an toàn cho Trang thông tin điện tử/ Cổng thông tin điện tử (gọi tắt là trang web):

a) Xác định cấu trúc thiết kế trang web: Quản lý toàn bộ các phiên bản của mã nguồn, phối hợp với đơn vị thực hiện dịch vụ hosting tổ chức mô hình trang web hợp lý tránh khả năng tấn công leo thang đặc quyền. Yêu cầu đơn vị cung cấp dịch vụ hosting phải cài đặt các hệ thống phòng vệ như tường lửa (firewall), thiết bị phát hiện/phòng chống xâm nhập (IDS/IPS) ở mức ứng dụng web (WAF- Web Application Firewall).

b) Thiết lập và cấu hình cơ sở dữ liệu an toàn:

- Luôn cập nhật bản vá lỗi mới nhất cho hệ quản trị cơ sở dữ liệu; sử dụng công cụ để đánh giá, tìm kiếm lỗ hổng trên máy chủ cơ sở dữ liệu;

- Gỡ bỏ các cơ sở dữ liệu không sử dụng;

- Có các cơ chế sao lưu dữ liệu, tài liệu hóa quá trình thay đổi cấu trúc bằng cách xây dựng nhật ký CSDL với các nội dung như: nội dung thay đổi, lý do thay đổi, thời gian, vị trí thay đổi,...

8. Thiết lập cơ chế sao lưu và phục hồi máy chủ, máy trạm

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 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 backup mới nhất để hệ thống hoạt động.

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

Điều 6. Trách nhiệm của Lãnh đạo đơn vị

1. Khi có sự cố hoặc nguy cơ mất an toàn thông tin, kịp thời áp dụng mọi biện pháp để khắc phục và hạn chế thiệt hại; ưu tiên sử dụng lực lượng kỹ thuật an ninh thông tin của đơn vị.

Trường hợp có sự cố nghiêm trọng vượt quá khả năng khắc phục của đơn vị, phải báo cáo ngay cho Sở Thông tin và Truyền thông để cùng phối hợp xử lý.

2. Tạo điều kiện thuận lợi cho các cơ quan chức năng tham gia khắc phục sự cố và thực hiện đúng theo hướng dẫn.

3. 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 về an toàn thông tin.

Điều 7. Trách nhiệm của cán bộ công chức trong các cơ quan, đơn vị quản lý hành chính nhà nước.

1. Nghiêm chỉnh chấp hành các quy chế nội bộ, quy trình về an toàn, an ninh thông tin của Sở cũng như quy định khác của pháp luật, nâng cao ý thức cảnh giác và trách nhiệm bảo đảm an toàn, an ninh thông tin tại đơn vị.

2. Khi phát hiện sự cố phải báo ngay với cơ quan cấp trên và bộ phận chuyên trách CNTT để kịp thời ngăn chặn, xử lý.

3. Hưởng ứng, tham gia các chương trình đào tạo, hội nghị về an toàn, an ninh thông tin do các cấp tổ chức.

CHƯƠNG IV
KHEN THƯỞNG, XỬ LÝ VI PHẠM

Điều 8. Khen thưởng

Các phòng, ban, đơn vị trực thuộc; công chức, người lao động thực hiện tốt Quy chế này đem lại hiệu quả thiết thực sẽ được xem xét đánh giá khen thưởng.

Điều 9. Xử lý vi phạm

Các phòng, ban, đơn vị trực thuộc; công chức, 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.

CHƯƠNG V
ĐIỀU KHOẢN THI HÀNH

Điều 10. Trong quá trình thực hiện nếu có phát sinh khó khăn, vướng mắc cần sửa đổi, bổ sung các phòng ban, đơn vị kịp thời báo cáo về Văn phòng Sở tổng hợp trình Lãnh đạo sở xem xét, giải quyết.