UBND TỈNH BÌNH PHƯỚC
SỞ KẾ HOẠCH VÀ ĐẦU TƯ

Số: 995/QyĐ-SKHĐT

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

Bình Phước, ngày 21 tháng 8 năm 2014.

QUY ĐỊNH
Về việc đảm bảo an toàn, an ninh thông tin điện tử; khuyến khích ứng dụng phần mềm nguồn mở; sử dụng an toàn hệ thống hộp thư điện tử công vụ thuộc Sở Kế hoạch và Đầu tư Bình Phước

Chương I
QUY ĐỊNH ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN ĐIỆN TỬ; KHUYẾN KHÍCH ỨNG DỤNG PHẦN MỀM NGUỒN MỞ

Điều 1. Đảm bảo an toàn mạng và hạ tầng kỹ thuật

1. Phòng máy chủ:

Phòng máy chủ phải đảm bảo các điều kiện cho những thiết bị đặt trong đó hoạt động ổn định, các điều kiện tối thiểu gồm: được bố trí ở khu vực có điều kiện an ninh, tốt; khô ráo, có điều hòa không khí.

2. Thiết lập các cơ chế bảo vệ mạng nội bộ:

a) Khi có kết nối mạng nội bộ với mạng ngoài (như: internet, mạng cơ quan khác,...) cần sử dụng hệ thống phòng thủ, bảo vệ mạng nội bộ (như: thiết bị tường lửa chuyên dụng, phần mềm tường lửa, ...);

b) Hệ thống mạng không dây (Wifi) phải được thiết lập mật khẩu truy cập đủ mạnh và phân lớp mạng riêng cho các máy tính truy cập mạng không dây, định kỳ thay đổi mật khẩu, chậm nhất ba tháng phải đổi một lần;

c) Thiết lập, cấu hình đầy đủ các tính năng của thiết bị an toàn mạng. Thường xuyên kiểm tra nhằm kịp thời phát hiện những dấu hiệu bất thường gây mất an toàn cho hệ thống mạng nội bộ của cơ quan, đơn vị;

d) Kiểm soát chặt chẽ việc cài đặt các phần mềm lên các máy chủ và máy trạm

g) Theo dõi thường xuyên tình trạng lây nhiễm và thực hiện loại bỏ phần mềm độc hại khỏi hệ thống thông tin.

3. An toàn cho máy tính cá nhân:

a) Kích hoạt và thiết lập chế độ tự động cập nhật bản vá lỗ hổng bảo mật cho các phần mềm trên mỗi máy tính cá nhân; đặt mật khẩu đăng nhập, chế độ bảo vệ màn hình cho máy tính cá nhân nhằm hạn chế các nguy cơ xâm nhập trái phép.

b) Cài đặt phần mềm phòng, chống virus, mã độc cho tất cả các máy tính trong mạng nội bộ của cơ quan.

c) Không cài đặt phần mềm không rõ nguồn gốc, xuất xứ; không truy cập những trang web có nội dung không lành mạnh, không mở những thư điện từ không rõ địa chỉ người gửi,...;

d) Hạn chế sử dụng chức năng chia sẻ thư mục (Sharing). Khi sử dụng chức năng này thiết lập cơ chế chỉ đọc (Read Only) đối với những thư mục được chia sẻ trong mạng nội bộ. Chỉ sử dụng cơ chế cho phép toàn quyền đọc, ghi (Read, Write) khi thật cần thiết yêu cầu phải sử dụng mật khẩu khi truy cập thư mục chia sẻ và thực hiện thu hồi chức năng này sau khi đã sử dụng xong.

4. An toàn cho máy chủ:

a) Khi cần kết nối từ xa, nhất là từ Internet vào máy chủ để quản trị, phải sử dụng phương thức kết nối có mã hóa (ví dụ: SSH, VPN,...);

b) Các máy chủ chỉ dùng để cài đặt các phần mềm, dịch vụ dùng chung của cơ quan; không cài đặt các phần mềm không rõ nguồn gốc, phần mềm không có nhu cầu sử dụng. Không sử dụng máy chủ để duyệt web đọc báo, xem tin tức, chơi điện tử,...

c) Cài đặt phần mềm phòng, chống virus, mã độc cho tất cả các máy chủ, đồng thời đảm bảo các phần mềm phòng, chống virus, mã độc này luôn được cập nhật khả năng nhận dạng virus, mã độc mới từ nhà sản xuất.

5. An toàn khi sử dụng các thiết bị lưu trữ ngoài:

a) Việc sử dụng các thiết bị lưu trữ ngoài như ổ cứng di động, các loại thẻ nhớ, thiết bị lưu trữ USB,... phải quét virus trước khi đọc hoặc sao chép dữ liệu;

b) Hạn chế tối đa việc sử dụng các thiết bị lưu trữ ngoài để sao chép, di chuyển dữ liệu.

Điều 2. An toàn dữ liệu, cơ sở dữ liệu và phần mềm ứng dụng CNTT.

1. Ưu tiên ứng dụng phần mềm mã nguồn mở (cụ thể: phần mềm văn phòng OpenOffice, phần mềm thư điện tử Mozilla ThunderBird, phần mềm trình duyệt Web Mozilla FireFox, phần mềm gõ tiếng Việt Unikey, hệ điều hành mã nguồn mở Ubuntu) để khắc phục và hướng tới việc xóa bỏ việc vi phạm bản quyền phần mềm trong cơ quan, tiết kiệm chi phí bản quyền phần mềm đồng thời tạo sự thích nghi với các sản phẩm tương đương với các phần mềm thương mại mã nguồn đóng.

2. Các hệ thống phần mềm, cơ sở dữ liệu phải có cơ chế sao lưu dữ liệu dự phòng, dữ liệu được lưu trữ tại nơi an toàn, đồng thời phải thường xuyên kiểm tra để đảm bảo sẵn sàng phục hồi khi có sự cố xảy ra.

3. Sử dụng mật mã để bảo đảm an toàn và bảo mật dữ liệu trong lưu trữ và giao dịch theo quy định của Nhà nước về mật mã.

4. Quản lý chặt chẽ việc di chuyển các trang thiết bị CNTT lưu trữ dữ liệu, nhất là các thông tin thuộc danh mục bí mật Nhà nước.

5. Quản lý và phân quyền truy cập phần mềm và cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ của người sử dụng.

6. Phần mềm hệ quản trị cơ sở dữ liệu phải được thiết lập cơ chế tự động và thường xuyên cập nhật bản vá lỗ hổng bảo mật từ nhà sản xuất.

Điều 3. Đảm bảo an toàn trong hoạt động trao đổi thông tin trên mạng.

1. Việc gửi thông tin trên mạng phải đảm bảo:

a) Không giả mạo nguồn gốc của thông tin;

b) Tuân thủ quy định này và quy định của pháp luật có liên quan.

2. Phân loại tài sản thông tin theo các tiêu chí về giá trị, độ nhạy cảm và tầm quan trọng, tần suất sử dụng, thời gian lưu trữ.

3. Thực hiện các biện pháp quản lý phù hợp với từng loại tài sản thông tin đã phân loại.

4. Khuyến khích áp dụng công nghệ mã hóa, chữ ký số,... khi chia sẻ, lưu trữ, trao đổi thông tin trên môi trường mạng.

Điều 4. Bảo vệ bí mật Nhà nước trong công tác ứng dụng CNTT.

1. Không được sử dụng máy tính nối mạng để soạn thảo văn bản, chuyển giao, lưu trữ thông tin có nội dung thuộc bí mật nhà nước; cung cấp tin, tài liệu và đưa thông tin bí mật nhà nước trên mạng

2. Không được in, sao chụp tài liệu bí mật nhà nước trên các thiết bị kết nối mạng.

3. Khi sửa chữa, khắc phục các sự cố của máy tính dùng soạn thảo văn bản mật, các cơ quan phải báo cáo và có sự giám sát, quản lý chặt chẽ của cơ quan có thẩm quyền.

4. Có biện pháp quản lý chặt chẽ trong việc sử dụng và thanh lý tài sản các trạng thiết bị CNTT lưu trữ các thông tin thuộc danh mục bí mật Nhà nước. Tuân thủ Pháp lệnh bảo vệ bí mật Nhà nước và các quy định khác có liên quan của Nhà nước về công tác bảo vệ bí mật nhà nước.

Điều 5. Trách nhiệm của CBCCVC trong các cơ quan, đơn vị.

1. Trách nhiệm của cán bộ chuyên trách, phụ trách CNTT:

a) Chịu trách nhiệm xây dựng, triển khai các biện pháp quản lý vận hành, quản lý kỹ thuật, xây dựng phương án hạn chế, khắc phục các rủi ro và nguy cơ có thể xảy ra, tham mưu xây dựng quy định về đảm bảo an toàn cho hệ thống thông tin của cơ quan, theo Quy định này và các quy định có liên quan khác của Nhà nước;

b) Phối hợp với các cá nhân của phòng ban có liên quan trong việc kiểm tra, phát hiện và khắc phục các sự cố mất an toàn, an ninh thông tin tại cơ quan.

c) Trực tiếp thiết lập các biện pháp kỹ thuật đảm bảo an toàn cho các máy tính cá nhân trong cơ quan; hướng dẫn các CBCCVC của cơ quan tuân thủ các biện pháp đảm bảo an toàn, an ninh thông tin trong khai thác, sử dụng phần mềm và các trang thiết bị CNTT.

2. Trách nhiệm của CBCCVC:

a) Thường xuyên cập nhật và chấp hành nghiêm túc những chính sách, các quy định về an toàn, an ninh thông tin theo Quy định này và của cơ quan, cũng như các quy định khác của pháp luật. Nâng cao ý thức cảnh giác và trách nhiệm đảm bảo an toàn, an ninh thông tin tại cơ quan. Thực hiện những hướng dẫn về an toàn, an ninh thông tin của cán bộ chuyên trách, phụ trách CNTT.

b) Khi phát hiện sự cố gây mất an toàn, an ninh thông tin phải báo ngay với cấp trên và cán bộ chuyên trách, phụ trách CNTT để kịp thời ngăn chặn, xử lý.

Chương II
SỬ DỤNG AN TOÀN HỆ THỐNG HỘP THƯ ĐIỆN TỬ CÔNG VỤ

Điều 6. Trách nhiệm của người sử dụng hộp thư điện tử công vụ:

Các cán bộ, công chức, viên chức của cơ quan được tỉnh cấp hộp thư điện tử có đuôi ***@binhphuoc.gov.vn*** có trách nhiệm:

1. Phải tuân thủ theo các quy định về cách sử dụng mật khẩu cho hộp thư điện tử.

2. Bảo vệ mật khẩu sử dụng thư điện tử.

3. Quản lý và lưu trữ các thư điện tử của cá nhân.

4. Chịu trách nhiệm về nội dung thông tin của mình gửi lên mạng.

5. Không truy nhập vào hộp thư của người khác và không để người khác sử dụng địa chỉ, hộp thư điện tử của mình.

6. Không được cung cấp mật khẩu hoặc để lộ mật khẩu đăng nhập vào hệ thống thư điện tử cho người khác.

7. Không phát tán thư rác hoặc trao đổi thông tin trái với quy định qua hộp thư điện tử đã được cấp.

8. Thường xuyên kiểm tra hộp thư để lưu trữ những thư quan trọng về máy và xóa các thư không cần thiết (thư rác, thư quảng cáo).

9. Khi gặp sự cố về hộp thư điện tử phải thông báo cho người phụ trách công nghệ thông tin của cơ quan để hướng dẫn và xử lý kịp thời.

Chương III
ĐIỀU KHOẢN THI HÀNH

Điều 7. Tổ chức thực hiện

- Quy định này có hiệu lực kể từ ngày ký. Các CBCC, VC trong cơ quan có trách nhiệm thực hiện đúng quy định này.

- Bộ phận Tin học – Văn phòng Sở có trách nhiệm hướng dẫn, giải thích và tổ chức thực hiện việc thi hành quy định này đến toàn thể CBCC, VC.

- Bản quy định có thể được Giám đốc bổ sung, sửa đổi khi cần thiết theo đề nghị Bộ phận Tin học Văn phòng Sở./.

Nơi nhận:
- *Toàn thể CBCC, VC;*
- *Lưu: VT.*

GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ KẾ HOẠCH VÀ ĐẦU TƯ
TỈNH BÌNH PHƯỚC

Vũ Thành Nam