UBND TỈNH ĐĂK NÔNG
SỞ KHOA HỌC VÀ CÔNG NGHỆ

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

Số: 181 /QĐ-SKHCN

Đăk Nông, ngày 17 tháng 11 năm 2016

QUYẾT ĐỊNH

Ban hành Quy chế đảm bảo an toàn thông tin
trong quản lý, vận hành và khai thác hệ thống thông tin

GIÁM ĐỐC SỞ KHOA HỌC VÀ CÔNG NGHỆ

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

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; 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 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 Thông tư số 23/2011/TT-BTTTT ngày 11/3/2011 của 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 Quyết định số 28/2010/QĐ-UBND ngày 28/9/2010 của Ủy ban nhân dân tỉnh Đắk Nông về việc ban hành quy chế đảm bảo an toàn, an ninh thôn gtin trong lĩnh vực ứng dụng công nghệ thông tin của các cơ quan, đơn vị quản lý hành chính nhà nước trên địa bàn tỉnh Đắk Nông;

Theo đề nghị của Chánh Văn phòng Sở Khoa học và Công nghệ,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế đảm bảo an toàn thông tin trong quản lý, vận hành và khai thác hệ thống thông tin của Sở Khoa học và Công nghệ tỉnh Đăk Nông.

Điều 2. Chánh Văn phòng Sở, Lãnh đạo các phòng, đơn vị trực thuộc và toàn thể cán bộ, công chức, viên chức thuộc Sở Khoa học và Công nghệ có trách nhiệm thi hành Quyết định này.

Quyết định có hiệu lực kể từ ngày ký./.

Nơi nhận:
- GĐ và các PGĐ Sở;
- Như Điều 2;
- Lưu VT,VP.

GIÁM ĐỐC

Phạm Ngọc Danh

QUY CHẾ

Đảm bảo an toàn thông tin trong quản lý, vận hành và khai thác hệ thống thông tin của Sở Khoa học và Công nghệ

(Ban hành kèm theo Quyết định số 181/QĐ-SKHCN. ngày 17 tháng 11 năm 2016 Giám đốc Sở Khoa học và Công nghệ tỉnh Đắk Nông)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi, đối tượng áp dụng

Quy chế này bao gồm các điều kiện tối thiểu phải tuân thủ nhằm đảm bảo an toàn thông tin trong quản lý, vận hành và khai thác hệ thống thông tin của Sở Khoa học và Công nghệ; thông tin được đảm bảo an toàn bao gồm các thông tin thuộc Sở hoặc được gửi đến Sở từ Bộ Khoa học và Công nghệ, các cơ quan, đơn vị khác; cán bộ, công chức tham gia quản lý; cán bộ, công chức, và các đối tượng tham gia vận hành và khai thác hệ thống thông tin.

Điều 2. Giải thích từ ngữ

1. "Đảm bảo an toàn thông tin" là đảm bảo tính bí mật, tính toàn vẹn và tính sẵn sàng của thông tin, trong đó:

a) Tính bí mật: thông tin không bị tiết lộ tới các đối tượng không có thẩm quyền đối với thông tin.

b) Tính toàn vẹn: thông tin không bị sửa đổi làm sai lệch nội dung.

c) Tính sẵn sàng: thông tin cung cấp được tới đối tượng sử dụng có thẩm quyền đối với thông tin.

2. "Hệ thống mạng Sở Khoa học và Công nghệ": Hệ thống mạng máy tính của Sở Khoa học và Công nghệ bao gồm hạ tầng truyền thông (máy tính, thiết bị kết nối đến Bộ Khoa học và Công nghệ) và hệ thống kết nối ra môi trường bên ngoài (máy tính, thiết bị kết nối ra môi trường internet).

3. "Mật khẩu phức tạp": là mật khẩu đáp ứng yêu cầu sau:

- Có tối thiểu 8 ký tự.

- Gồm tối thiểu 3 trong số 4 loại ký tự sau: chữ cái viết hoa (A-Z), chữ cái viết thường (a-z), chữ số (0-9), các ký tự khác trên bàn phím máy tính (~, !, ...)

4 ."Thuật toán mã hóa an toàn" là thuật toán mã hóa theo tiêu chuẩn Việt Nam hoặc thế giới mà tại thời điểm áp dụng chưa có công bố thuật toán đó đã bị giải hoặc nếu có khả năng giải thì thời gian giải thuật toán này dài hơn thời gian dữ liệu cần được bảo vệ dưới dạng mã hóa.

5. "Bí mật nhà nước": thông tin thuộc Danh mục Bí mật Nhà nước cấp độ tuyệt mật, tối mật, mật của ngành Khoa học và Công nghệ theo quy định hiện hành và bí mật nhà nước của các cơ quan, đơn vị khác gửi đến Sở Khoa học và Công nghệ

6. "Người dùng": cán bộ, công chức, viên chức, nhân viên hợp đồng của Sở được sử dụng máy tính tại đơn vị để xử lý công việc.

Điều 3. Nguyên tắc chung về đảm bảo an toàn thông tin

1. Việc bảo đảm an toàn thông tin là yêu cầu bắt buộc trong quá trình tạo lập, xử lý, sử dụng thông tin và quá trình thiết kế, xây dựng, vận hành, nâng cấp, hủy bỏ các hạ tầng kỹ thuật công nghệ thông tin.

2. Người dùng thực hiện các công đoạn liên quan đến thông tin nêu tại mục 1 điều này có trách nhiệm đảm bảo an toàn thông tin theo quy định của Nhà nước và của Sở Khoa học và Công nghệ.

3. Người dùng phải có những kiến thức cơ bản về an toàn thông tin trên môi trường máy tính, mạng máy tính phù hợp với công việc được phân công.

4. Thông tin thuộc danh mục bí mật nhà nước trên môi trường máy tính và mạng máy tính phải được bảo vệ theo các quy định của Nhà nước, Quy chế bảo vệ bí mật nhà nước của ngành Khoa học và Công nghệ và các nội dung tương ứng trong quy định này.

Chương II:
QUY ĐỊNH CỤ THỂ

Điều 4. Đảm bảo an toàn mức vật lý

1. Các khu vực sau phải được kiểm soát truy cập vật lý để phòng tránh truy cập trái phép hoặc sai mục đích: Phòng máy chủ và thiết bị lưu trữ, các tủ mạng và đấu nối, thiết bị nguồn điện và dự phòng điện khẩn cấp, các phòng vận hành, kiểm soát (quản trị) hệ thống. Chỉ có các cán bộ chuyên trách mới được phép vào khu vực này, cá nhân khác nhất thiết phải được sự đồng ý của cán bộ công nghệ thông tin (CNTT) chuyên trách, đồng thời phải cán bộ chuyên trách CNTT cùng vào.

2. Người dùng sử dụng các thiết bị lưu trữ dữ liệu di động (máy tính xách tay, thiết bị số cầm tay, thẻ nhớ USB, ổ cứng ngoài, băng từ...) để lưu thông tin thuộc phạm vi bảo vệ quy định tại Điều 1 có trách nhiệm bảo vệ các thiết bị này và thông tin lưu trên thiết bị, tránh làm mất, lộ thông tin. Không mang ra nước ngoài thông tin của cơ quan, Nhà nước không liên quan tới nội dung công việc thực hiện ở nước ngoài. Nghiêm cấm sử dụng thiết bị do cá nhân tự trang bị để lưu giữ bí mật Nhà nước.

3. Các thiết bị lưu trữ dữ liệu không sử dụng tiếp cho công việc của Sở (thanh lý, cho, tặng) phải được xóa nội dung bằng phần mềm hoặc bằng thiết bị hủy dữ liệu chuyên dụng hay phá hủy vật lý.

Điều 5. Đảm bảo an toàn máy tính làm việc

1. Máy tính phục vụ công việc (bao gồm máy chủ và máy tính phục vụ công việc của người dùng):

a) Máy tính làm việc của cán bộ, công chức phải được cập nhật bản vá lỗi hệ điều hành về an ninh, cài đặt phần mềm phòng, diệt virus và cập nhật mẫu phát hiện virus gần nhất.

b) Bộ phận công nghệ thông tin của Sở chịu trách nhiệm cài đặt hệ điều hành, phần mềm cho máy tính phục vụ công việc. Người dùng không được can thiệp (cài đặt mới, thay đổi, gỡ bỏ,...) các phần mềm đã cài đặt trên máy tính khi chưa được sự đồng ý của bộ phận công nghệ thông tin của Sở.

c) Đối với các máy tính có chứa dữ liệu quan trọng của ngành, nhà nước: Người dùng phải thực hiện thao tác khóa máy tính (sử dụng tính năng cài đặt sẵn trên máy) khi rời khỏi nơi đặt máy tính và tắt máy tính khi rời khỏi cơ quan.

2. Nghiêm cấm máy tính của cá nhân chưa cài đặt phần mềm phòng diệt virus và cập nhật mẫu phát hiện virus kết nối vào hệ thống mạng nội bộ khi chưa có sự đồng ý của cán bộ CNTT Sở.

Điều 6. Đảm bảo an toàn hệ thống mạng máy tính

1. Hệ thống mạng phải được bảo vệ bằng tường lửa đáp ứng các yêu cầu sau:

a) Phân chia hệ thống mạng thành các vùng mạng theo phạm vi truy cập và kiểm soát truy cập giữa các vùng bằng tường lửa.

b) Vô hiệu hóa tất cả các dịch vụ không sử dụng tại từng vùng mạng;

c) Che giấu và tránh truy cập trực tiếp các địa chỉ mạng bên trong từ bên ngoài (Internet, hạ tầng truyền thông ngành Khoa học và Công nghệ).

d) Cài đặt các bản cập nhật, vá lỗi đúng hạn cho các tường lửa để khắc phục các điểm yếu an ninh nghiêm trọng; Có chế độ bảo hành hoặc thiết bị dự phòng để đảm bảo sự hoạt động liên tục của tường lửa.

3. Mạng nội bộ của Sở phải được giám sát bởi hệ thống phát hiện và phòng chống tấn công.

4. Mạng wifi phải được bảo vệ tránh bị tiếp cận trái phép.

5. Đối với truy cập từ xa vào hệ thống mạng nội bộ:

a) Máy tính dùng để kết nối tới mạng của Sở phải được đảm bảo an toàn theo quy định tại Điều 5; người dùng kết nối phải được sự cho phép của cán bộ chuyên trách CNTT sở.

b) Kết nối truy cập từ xa phải sử dụng mã hóa kênh truyền;

c) Truy cập từ xa cho mục đích quản trị hệ thống phải áp dụng xác thực tối thiểu 2 nhân tố.

Điều 7. Đảm bảo an toàn kết nối Internet

1. Áp dụng các biện pháp cần thiết để đảm bảo an toàn thông tin trong hoạt động kết nối Internet của người dùng, tối thiểu đáp ứng yêu cầu sau:

a) Có tường lửa kiểm soát truy cập Internet.

b) Có chế độ hỗ trợ lọc bỏ, không cho phép truy cập các trang tin có nghi ngờ chứa mã độc hoặc các nội dung không phù hợp (phản động hoặc trái thuần phong mỹ tục).

c) Máy tính chứa dữ liệu quan trọng hoặc có khả năng tiếp cận các dữ liệu, ứng dụng quan trọng của ngành Khoa học và Công nghệ không được

mở trang tin hoặc ứng dụng Internet trực tiếp trên máy này; chỉ được phép truy cập vào các trang tin trên Internet phục vụ công việc của Sở.

d) Người dùng không được sử dụng các thiết bị của cá nhân (modem 3G, điện thoại di động,...) để kết nối máy tính làm việc vào Internet khi chưa được sự đồng ý của bộ phận công nghệ thông tin.

2. Đối với máy chủ và thiết bị công nghệ thông tin khác, chỉ thiết lập kết nối Internet cho các hệ thống cần phải có giao tiếp với Internet (các máy chủ, thiết bị cung cấp giao diện ra Internet của trang tin điện tử, thư điện tử; thiết bị cập nhật bản vá hệ điều hành, mẫu phòng diệt virus, các mẫu lỗ hổng bảo mật, mẫu tấn công,...).

3. Nghiêm cấm máy tính dùng để soạn thảo, in ấn, lưu trữ bí mật Nhà nước kết nối Internet hoặc nếu kết nối internet (vì một lý do nào đó) cần phải thực hiện mã hóa tài liệu và đặt mật khẩu phức tạp trong quá trình làm việc.

Điều 8. Đảm bảo an toàn mức ứng dụng

1. Yêu cầu về đảm bảo an toàn thông tin phải được đưa vào tất cả các công đoạn liên quan đến ứng dụng (thiết kế, xây dựng, triển khai và vận hành, sử dụng,...).

2. Ứng dụng phải đáp ứng yêu cầu sau:

- Mã hóa thông tin bí mật hoặc nhạy cảm bằng thuật toán mã hóa an toàn.

- Kiểm tra tính hợp lệ của dữ liệu đầu vào và đầu ra để đảm bảo dữ liệu chính xác và phù hợp.

- Thực hiện các quy trình kiểm soát việc cài đặt phần mềm trên các máy chủ, máy tính của người dùng, thiết bị mạng đang hoạt động thuộc hệ thống mạng nội bộ.

- Hạn chế truy cập tới mã nguồn chương trình và phải đặt mã nguồn trong môi trường an toàn do bộ phận chuyên trách quản lý.

- Thực hiện kiểm tra phát hiện và khắc phục lỗ hổng bảo mật của ứng dụng trước khi đưa vào sử dụng và định kỳ tối thiểu 6 tháng một lần trong quá trình sử dụng.

3. Đối với ứng dụng mua ở dạng đóng gói:

- Theo dõi nắm bắt thông tin về các lỗ hổng bảo mật mới và cập nhật thường xuyên bản vá lỗi về an ninh, cho ứng dụng.

- Trường hợp lỗ hổng đã được phát hiện mà chưa có bản vá lỗi của đơn vị sản xuất phần mềm, phải thực hiện đánh giá rủi ro và có biện pháp phòng tránh phù hợp.

Điều 9. Đảm bảo an toàn mức dữ liệu

1. Các nội dung mật, quan trọng hoặc nhạy cảm khi lưu trữ trên thiết bị di động hoặc truyền nhận trên hệ thống mạng phải được mã hóa, trong đó:

Chương III

TRÁCH NHIỆM ĐẢM BẢO AN TOÀN AN NINH THÔNG TIN

Điều 15. Trách nhiệm của bộ phận chuyên trách CNTT

1. Thường xuyên theo dõi, kiểm tra hệ thống thông tin của đơn vị.

2. Khi có sự cố hoặc nguy cơ mất an toàn, an ninh thông tin cần kịp thời áp dụng mọi biện pháp để khắc phục và hạn chế mọi thiệt hại, sau đó lập biên bản báo cáo bằng văn bản cho lãnh đạo cấp trên trực tiếp quản lý và Sở Thông tin và Truyền thông.

Trường hợp sự cố nghiêm trọng vượt quá khả năng khắc phục của đơn vị cần báo ngay cho lãnh đạo cấp trên trực tiếp quản lý và Sở Thông tin và Truyền thông.

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

4. Phối hợp với Đoàn kiểm tra (nếu có) để triển khai công tác kiểm tra khắc phục sự cố diễn ra nhanh chóng và đạt hiệu quả; Đồng thời cung cấp đầy đủ các thông tin khi Đoàn kiểm tra yêu cầu xuất trình.

Điều 16. Trách nhiệm của Văn phòng Sở

1. Theo dõi, đôn đốc việc thực hiện Quy chế.

2. Phối hợp với bộ phận chuyên trách CNTT thực hiện Khoản 2,3,4 của Điều 15 Chương này.

3. Tổng hợp các vướng mắc đề nghị bổ sung, chỉnh sửa quy chế; tham mưu đề xuất đầu tư kinh phí nâng cấp phần mềm, thiết bị và hạ tầng kỹ thuật để thực hiện tốt công tác an toàn thông tin trong quản lý, vận hành và khai thác hệ thống thông tin của đơn vị.

Điều 17. Trách nhiệm của cán bộ, công chức

1. Nghiêm chỉnh tuân thủ các quy định của Quy chế này và các quy định nội bộ cũng như các quy định khác của pháp luật, nâng cao ý thức cảnh giác, trách nhiệm đảm bảo an toàn thông tin tại cơ quan; không được xâm phạm an toàn thông tin của tổ chức, cá nhân khác.

2. Khi phát hiện sự cố phải báo cáo ngay với cơ quan cấp trên và bộ phận chuyên trách 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 khi có tổ chức.

GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ KHOA HỌC VÀ CÔNG NGHỆ
TỈNH ĐẮK NÔNG

Phạm Ngọc Danh