UBND TỈNH BÌNH ĐỊNH
SỞ KHOA HỌC VÀ CÔNG NGHỆ

Số: 112a/QĐ-SKHCN

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

Bình Định, ngày 10 tháng 4 năm 2019

QUYẾT ĐỊNH
Về việc ban hành Quy chế giám sát an toàn thông tin của Sở Khoa học và Công nghệ

GIÁM ĐỐC SỞ KHOA HỌC VÀ CÔNG NGHỆ

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

Căn cứ Luật An toàn thông tin mạng ngày 19/11/2015;

Căn cứ Quyết định số 22/2012/QĐ-UBND ngày 12/7/2012 của Ủy ban nhân dân 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 hành chính nhà nước tỉnh Bình Định;

Căn cứ Quyết định số 157/QĐ-UBND ngày 18/01/2016 của UBND tỉnh Bình Định về việc ban hành Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Khoa học và Công nghệ;

Xét đề nghị của Trưởng phòng Quản lý chuyên ngành,

QUYẾT ĐỊNH:

Điều 1. Ban hành "Quy chế giám sát an toàn thông tin của Sở Khoa học và Công nghệ".

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

Điều 3. Chánh Văn phòng, Trưởng các phòng và Lãnh đạo các đơn vị chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như điều 3;
- Lãnh đạo Sở;
- Lưu VP,VT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ KHOA HỌC VÀ CÔNG NGHỆ
TỈNH BÌNH ĐỊNH

Nguyễn Hữu Hà

UBND TỈNH BÌNH ĐỊNH
SỞ KHOA HỌC VÀ CÔNG NGHỆ

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

QUY CHẾ
Giám sát an toàn thông tin của Sở Khoa học và Công nghệ

(Ban hành kèm theo Quyết định số 1120/QĐ-SKHCN ngày 10/4/2019 của Giám đốc Sở Khoa học và Công nghệ)

Chương I
NHỮNG QUY ĐỊNH CHUNG

Điều 1. Mục đích giám sát an toàn, an ninh thông tin

1. Giảm thiểu được các nguy cơ gây sự cố mất an toàn thông tin (ATTT) và đảm bảo an ninh thông tin trong quá trình tác nghiệp của cán bộ, công chức, viên chức.

2. Công tác giám sát an toàn, an ninh thông tin là một trong những nhiệm vụ trọng tâm để đảm bảo việc ứng dụng công nghệ thông tin (CNTT) trong hoạt động của Sở được quản lý tốt.

Điều 2. Phạm vi, đối tượng áp dụng

Quy chế này áp dụng đối với tất cả các cán bộ, công chức viên chức của các phòng và các đơn vị trực thuộc Sở Khoa học và Công nghệ khi tham gia khai thác, sử dụng hệ thống công nghệ thông tin của Sở.

Chương II
QUY ĐỊNH GIÁM SÁT AN TOÀN, AN NINH THÔNG TIN

Điều 3. Các biện pháp giám sát an toàn, an ninh thông tin

1. Đối với Lãnh đạo Sở:

a. Chỉ đạo việc giám sát hệ thống thông tin của Sở. Thường xuyên kiểm tra, cập nhật các báo cáo của phòng chuyên môn quản lý công nghệ thông tin.

b. Xác định và phân bổ kinh phí chi thường xuyên cần thiết cho các hoạt động liên quan đến việc giám sát hệ thống thông tin.

2. Đối với cán bộ chuyên trách công nghệ thông tin tại Sở:

a. Tham mưu cho lãnh đạo phòng, lãnh đạo Sở về việc giám sát hệ thống thông tin tại Sở. Thường xuyên tự cập nhật các kiến thức về giám sát thông tin, nguy cơ tiềm ẩn có thể gây mất mát thông tin và các biện pháp phòng tránh khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ.

b. Thường xuyên cập nhật cấu hình chuẩn cho các thành phần của hệ thống thông tin, thiết lập cấu hình chặt chẽ nhất cho các sản phẩm an toàn thông tin nhưng vẫn duy trì yêu cầu hoạt động của hệ thống thông tin.

c. Thường xuyên thực hiện việc theo dõi bản ghi nhật ký hệ thống và các sự việc khác có liên quan để giám sát, báo cáo các nguy cơ mất an toàn của hệ thống thông tin có thể xảy ra do sự truy cập trái phép, sử dụng trái phép, mất, thay đổi hoặc phá hủy thông tin và hệ thống thông tin.

d. Kiểm soát chặt chẽ việc cài đặt phần mềm vào máy trạm và máy chủ.

3. Đối với cán bộ, công chức, viên chức:

a. Thường xuyên cập nhật, thực hiện những chính sách, thủ tục an toàn thông tin của Sở.

b. Giám sát việc cài đặt phần mềm trên máy tính do mình sử dụng.

c. Kiểm tra các tập tin đính kèm theo thư điện tử, quét virus trước khi mở, không được mở các thư điện tử có tập tin đính kèm có nguồn gốc không rõ ràng vì rất có thể có virus, phần mềm gián điệp được đính kèm theo thư.

e. Phải đặt mật khẩu truy nhập vào máy tính của mình, đồng thời thiết lập chế độ bảo vệ tắt màn hình có sử dụng mật khẩu bảo vệ sau một khoảng thời gian nhất định không sử dụng máy tính. Sử dụng các thiết bị lưu trữ (usb, ổ cứng gắn ngoài...) an toàn, đúng cách để phòng ngừa virus, phần mềm gián điệp xâm nhập máy tính: khi gắn thiết bị lưu trữ vào máy tính, không được trực tiếp truy cập ngay mà phải quét virus trước.

Điều 4. Các biện pháp quản lý kỹ thuật cho công tác giám sát 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.

2. Quản lý hệ thống mạng không dây: Khi thiết lập mạng không dây để kết nối với mạng cục bộ thông qua các điểm truy nhập (Access Point), cần thiết lập các tham số như: tên, SSID, mật khẩu, mã hóa dữ liệu và thông báo các thông tin liên quan đến Access Point để cơ quan sử dụng.

3. Tổ chức quản lý tài khoản của các hệ thống thông tin, bao gồm: Tạo mới, kích hoạt, sửa đổi, vô hiệu hóa và loại bỏ các tài khoản. Đồng thời tổ chức kiểm tra các tài khoản của hệ thống thông tin ít nhất 06 tháng/1 lần và triển khai các công cụ tự động để hỗ trợ việc quản lý các tài khoản của hệ thống thông tin. 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 (khóa, thẻ nhận dạng, thư mục lưu trữ,...) đối với cán bộ, nhân viên đã chuyển công tác, chấm dứt hợp đồng lao động.

4. Quản lý đăng nhập hệ thống: Các hệ thống thông tin cần giới hạn số lần đăng nhập sai liên tiếp. Hệ thống tự động khóa tài khoản hoặc cô lập 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. Tổ chức theo dõi và kiểm soát tất cả các phương pháp truy nhập từ xa tới hệ thống thông tin bao gồm cả sự truy nhập

có chức năng quản trị, tăng cường việc sử dụng mạng riêng ảo khi có nhu cầu làm việc từ xa; yêu cầu người sử dụng đặt mật khẩu với độ an toàn cao, giám sát, nhắc nhở khuyến cáo nên thay đổi thường xuyên mật khẩu. Hệ thống thông tin cần có cơ chế kiểm tra, cho phép ứng với mỗi phương pháp truy nhập từ xa và cơ chế tự động giám sát, điều khiển các truy nhập từ xa.

5. Quản lý Logfile: Hệ thống thông tin cần ghi nhận các sự kiện cần thiết phục vụ quá trình kiểm soát: quá trình đăng nhập hệ thống, các thao tác cấu hình hệ thống, quá trình truy xuất hệ thống; ghi nhận đầy đủ các thông tin trong các bản ghi nhật ký để xác định những sự kiện nào đã xảy ra, nguồn gốc và các kết quả của sự kiện để có cơ chế bảo vệ và lưu giữ nhật ký trong một khoảng thời gian nhất định.

6. 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 và hỗ trợ người sử dụng cài đặt các phần mềm này trên máy trạm. Thường xuyên cập nhật các phiên bản 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, phù hợp với quy trình và chính sách quản lý hệ thống thông tin của tổ chức, thiết lập chế độ quét thường xuyên ít nhất là hằng tuần.

7. Tổ chức quản lý tài nguyên: Kiểm tra, giám sát chức năng chia sẻ thông tin. Tổ chức cấp phát tài nguyên trên máy chủ theo danh mục thư mục cho từng phòng/ban; 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.

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

a. Đối với máy trạm, máy chủ: Thực hiện việc sao lưu dữ liệu như hệ điều hành, các phần mềm ứng dụng, phần mềm chuyên ngành, cơ sở dữ liệu chuyên môn, quan trọng phục vụ công tác của Sở bằng các phần mềm chuyên dụng; Cài đặt phần mềm diệt virus và phần mềm bức tường lửa.

b. Đối với máy chủ: Bảo đảm thiết lập cơ chế sao lưu và phục hồi hệ thống của máy chủ; Cơ chế bảo trì máy chủ định kỳ; Giám sát hiệu suất hoạt động của tài nguyên máy chủ nhằm phát hiện, ngăn chặn truy cập trái phép.

9. Có biện pháp ứng phó khi phát hiện hệ thống bị tấn công, thông qua các dấu hiệu như luồng tin tăng lên bất ngờ, nội dung trang chủ bị thay đổi, hệ thống hoạt động rất chậm khác thường.

10. Thống kê tình hình sử dụng hệ thống thư điện tử công vụ; thông tin truy cập trang thông tin điện tử; tài nguyên dữ liệu trên máy chủ; quản lý phần mềm quản lý ngành và cơ sở dữ liệu đề tài, dự án được.

11. Các giải pháp quản lý khác trong hoạt động giám sát:

a. Thiết lập cơ chế giám sát tự động tìm kiếm các lỗ hổng bảo mật trong hệ thống mạng gồm các lỗ hổng bảo mật trên các máy chủ, dịch vụ, ứng dụng đặc biệt là trên website.

b. Kiểm tra định kỳ các đối tượng trong mạng để phát hiện sớm các lỗ hổng bảo mật và đưa ra báo cáo, phương án xử lý kịp thời cho hệ thống mạng.

c. Trang bị các thành phần thiết bị mạng như firewall, switch, router.... đảm bảo các cấu hình không ở trạng thái mặc định và đã được tối ưu nhằm giảm thiểu các nguy cơ trong hệ thống mạng.

d. Phát hiện và phòng chống tấn công có chủ đích: Phân tích lưu lượng mạng để phát hiện các nguy cơ tấn công mạng, đặc biệt là các tấn công mạng có chủ đích.

Chương III
TRÁCH NHIỆM GIÁM SÁT AN TOÀN, AN NINH THÔNG TIN

Điều 5. Trách nhiệm của các phòng, đơn vị trực thuộc

1. Lãnh đạo các phòng, đơn vị trực thuộc Sở có trách nhiệm tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trước Lãnh đạo Sở trong công tác giám sát an toàn, an ninh thông tin của cơ quan, đơn vị mình.

2. Khi có sự cố hoặc nguy cơ mất an toàn thông tin phải kịp thời áp dụng mọi biện pháp để khắc phục và hạn chế thiệt hại, ưu tiên sử dụng lực lượng kỹ thuật an toàn, an ninh thông tin của cơ quan và lập biên bản, báo cáo bằng văn bản cho cơ quan cấp trên quản lý trực tiếp.

3. Phối hợp chặt chẽ với cơ quan Công an 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.

Điều 6. Trách nhiệm của cán bộ, công chức, viên chức

1. Trách nhiệm của cán bộ chuyên trách an toàn an ninh thông tin

a. Chịu trách nhiệm triển khai các biện pháp quản lý vận hành, quản lý kỹ thuật, tham mưu xây dựng các quy định giám sát an toàn, an ninh thông tin cho Hệ thống thông tin của Sở theo Quy chế này.

b. 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

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

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

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 7. Trách nhiệm thi hành

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

2. Quy chế này có hiệu lực kể từ ngày ban hành. Trong quá trình thực hiện nếu có những vấn đề vướng mắc, phát sinh thì phản ánh về phòng Quản lý Chuyên ngành để kịp thời báo cáo lãnh đạo Sở, đề nghị bổ sung hoàn thiện Quy chế./.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ KHOA HỌC VÀ CÔNG NGHỆ
TỈNH BÌNH ĐỊNH

Nguyễn Hữu Hà