UBND TỈNH KHÁNH HÒA
SỞ CÔNG THƯƠNG

Số: 142 /QĐ-SCT

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

Khánh Hòa, ngày 14 tháng 11 năm 2018

QUYẾT ĐỊNH
Về việc ban hành Quy định đảm bảo an toàn thông tin số trong hoạt động ứng dụng công nghệ thông tin của Sở Công Thương Khánh Hòa

GIÁM ĐỐC SỞ CÔNG THƯƠNG KHÁNH HÒA

Căn cứ Quyết định số 179/QĐ-UBND ngày 20/01/2016 của UBND tỉnh Khánh Hòa về việc kiện toàn chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức Sở Công Thương;

Căn cứ Quyết định số 38/2015/QĐ-UBND ngày 24/12/2015 của UBND tỉnh Khánh Hòa ban hành Quy định đảm bảo an toàn thông tin số trong hoạt động ứng dụng công nghệ thông tin trên địa bàn tỉnh Khánh Hòa;

Xét đề nghị của Chánh Văn phòng,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy định đảm bảo an toàn thông tin số trong hoạt động ứng dụng công nghệ thông tin của Sở Công Thương Khánh Hòa.

Điều 2. Quyết định này có hiệu lực kể từ ngày ký và thay thế Quyết định số 104/QĐ-SCT ngày 28/10/2015 của Sở Công Thương Khánh Hòa ban hành Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Sở Công Thương tỉnh Khánh Hòa.

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

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

GIÁM ĐỐC

Lê Thu Hải

UBND TỈNH KHÁNH HÒA
SỞ CÔNG THƯƠNG

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

QUY ĐỊNH
Đảm bảo an toàn thông tin số trong hoạt động ứng dụng công nghệ thông tin của Sở Công Thương Khánh Hòa

(Ban hành kèm theo Quyết định số: 142 /QĐ-SCT ngày 14 tháng 11 năm 2018 của Sở Công Thương Khánh Hòa)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh

Quy định này quy định việc đảm bảo an toàn thông tin số trong hoạt động ứng dụng công nghệ thông tin của Sở Công Thương Khánh Hòa.

2. Đối tượng áp dụng

Cán bộ, công chức và người lao động Sở Công Thương Khánh Hòa; các tổ chức và cá nhân có liên quan.

Điều 2. Mục tiêu và phương hướng thực hiện

1. Mục tiêu

Phòng ngừa, ngăn chặn nguy cơ gây mất an toàn thông tin số trong hoạt động ứng dụng công nghệ thông tin của Sở Công Thương Khánh Hòa theo quy định pháp luật.

2. Phương hướng thực hiện

Sử dụng mô hình mạng Domain để quản lý tập trung và tăng cường tính bảo mật cho hệ thống thông tin.

Điều 3. Giải thích từ ngữ

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

1. Hệ thống thông tin là hệ thống sử dụng công nghệ thông tin để thu thập, truyền, lưu trữ, xử lý và cung cấp thông tin phục vụ nhu cầu sử dụng của các tổ chức, cá nhân.

2. An toàn thông tin số là 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 tự nhiên hoặc do con người gây ra.

3. Công chức chuyên trách công nghệ thông tin: là công chức được giao trách nhiệm tham mưu công tác quản lý và trực tiếp thực hiện nhiệm vụ quản trị hệ thống thông tin.

Điều 4. Nguyên tắc chung

1. Hệ thống thông tin của Sở Công Thương tuân thủ nguyên tắc bảo đảm an toàn thông tin số theo quy định tại Điều 41 Nghị định số 64/2007/NĐ-CP ngày 10/04/2007 của Chính phủ về Ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước.

2. Giám đốc Sở là người có quyền cao nhất đối với toàn bộ hoạt động và công tác đảm bảo an toàn thông tin số cho hệ thống thông tin; có toàn quyền giao hay thu hồi quyền sử dụng hệ thống thông tin; có quyền quyết định việc sử dụng các thành phần của hệ thống thông tin ngoài mục đích phục vụ công việc trên cơ sở tuân thủ các quy định của pháp luật và chịu hoàn toàn trách nhiệm đối với quyết định của mình.

3. Cán bộ, công chức, người lao động tham gia sử dụng hệ thống thông tin Sở Công Thương phải tuân thủ quy định về kết nối và truy cập mạng Internet, sử dụng máy tính cá nhân trong hoạt động công vụ, quản lý và sử dụng tài khoản hệ thống thông tin được cấp, các quy định khác có liên quan đến an toàn, an ninh thông tin trên môi trường mạng do Sở Công Thương và UBND tỉnh ban hành.

Chương II
QUẢN LÝ HỆ THỐNG THÔNG TIN ĐẢM BẢO AN TOÀN THÔNG TIN SỐ

Điều 5. Nguyên tắc phân loại và mức độ ưu tiên quản lý các thành phần hệ thống thông tin

1. Nguyên tắc phân loại

Căn cứ thẩm quyền quản lý, sử dụng và phạm vi triển khai, phân loại như sau:

a) Các thành phần hệ thống thông tin do UBND tỉnh đầu tư và triển khai.

b) Các thành phần hệ thống thông tin do Sở Công Thương đầu tư sử dụng.

2. Mức độ ưu tiên quản lý

Các thành phần hệ thống thông tin do UBND tỉnh đầu tư sẽ được ưu tiên quản lý nhiều hơn vì ảnh hưởng trực tiếp và thường xuyên đến công tác quản lý quản lý nhà nước của Sở Công Thương.

Điều 6. Quản lý và điều hành hệ thống máy chủ, thiết bị mạng và thiết bị bảo vệ mạng

1. Phối hợp với Sở Thông tin và Truyền thông, đơn vị liên quan xây dựng tài liệu kỹ thuật mô tả kiến trúc hệ thống mạng, thông số kỹ thuật, cấu hình hệ thống, giải pháp sao lưu và phục hồi dữ liệu cho máy chủ, máy trạm, các thiết bị trong hệ thống thông tin để làm căn cứ quản lý, vận hành và xử lý sự cố.

2. Trang bị công cụ tường lửa và giám sát truy cập đối với hệ thống máy chủ, thiết bị mạng.

3. Thường xuyên cập nhật cấu hình chuẩn theo hướng dẫn, khuyến nghị của nhà sản xuất thiết bị, đơn vị cung cấp phần mềm ứng dụng hoặc cơ quan quản lý nhà nước chuyên ngành.

4. Hạn chế sử dụng các chức năng, cổng giao tiếp, giao thức và dịch vụ mạng không cần thiết nhưng vẫn đảm bảo duy trì hoạt động thường xuyên của hệ thống thông tin.

5. Kịp thời đầu tư nâng cấp hệ thống máy chủ, thiết bị mạng và thiết bị bảo vệ mạng khi xuất hiện tình trạng xuống cấp hoặc không còn khả năng đáp ứng được yêu cầu công việc hoặc không đảm bảo an toàn thông tin số trong hoạt động ứng dụng công nghệ thông tin.

Điều 7. Kiểm tra, rà soát và khắc phục sự cố hệ thống thông tin

1. Kiểm tra, rà soát toàn bộ hệ thống thông tin ít nhất 01 lần/năm để đánh giá, phát hiện các nguy cơ, khả năng gây mất an toàn thông tin số, từ đó thực hiện các biện pháp cần thiết và kịp thời để hạn chế thiệt hại ở mức thấp nhất cho hệ thống thông tin.

2. Phòng chống các phần mềm có hại như virus, worm, spyware,... cho hệ thống máy chủ, máy trạm và thiết bị mạng. Sao lưu cấu hình, trạng thái, ứng dụng, dữ liệu của hệ thống thông tin và lưu trữ dữ liệu sao lưu tại nơi an toàn. Dữ liệu sao lưu phải được kiểm tra và cập nhật thường xuyên để phục vụ công tác tra cứu, phục hồi trong trường hợp cần thiết.

3. Quản lý định danh đối với tất cả người dùng tham gia sử dụng hệ thống thông tin, chỉ cung cấp những chức năng thiết yếu nhất để phục vụ công việc; trang bị đầy đủ kiến thức bảo mật cần thiết cho người sử dụng trước khi cho phép truy cập và sử dụng hệ thống thông tin.

4. Quản lý các tài khoản của hệ thống thông tin; thực hiện hủy quyền truy cập và thu hồi các tài sản liên quan (khóa, thẻ tài khoản, thẻ nhận dạng,...) của người sử dụng đã nghỉ hưu, nghỉ việc hoặc chuyển công tác đến cơ quan khác nhưng vẫn đảm

bảo khả năng truy cập vào các hồ sơ, tài liệu được tạo ra bởi cán bộ, công chức hoặc nhân viên đó.

5. Theo dõi và ngăn chặn truy cập từ xa trái phép vào hệ thống thông tin; sử dụng chứng thực và mã hóa để ngăn chặn các truy cập mạng không dây có khả năng gây mất an toàn hệ thống thông tin.

6. Ghi nhận, lưu giữ quá trình đăng nhập, cấu hình, truy xuất hệ thống và các thông tin liên quan vào bản ghi nhật ký của hệ thống thông tin nhằm xác định những sự kiện đã xảy ra, nguồn gốc và kết quả các sự kiện đó, làm cơ sở để khắc phục các sự cố đã xảy ra.

7. Các biện pháp khác theo hướng dẫn của cơ quan quản lý chuyên ngành.

Chương III
SỬ DỤNG HỆ THỐNG THÔNG TIN ĐẢM BẢO AN TOÀN THÔNG TIN SỐ

Điều 8. Phân quyền sử dụng hệ thống thông tin

1. Giám đốc Sở quyết định việc phân quyền sử dụng các chức năng hệ thống thông tin đối với cá nhân tham gia sử dụng hệ thống tùy theo nhiệm vụ, chức trách được giao.

2. Tài khoản quản trị dùng để phân quyền sử dụng hệ thống thông tin được giao cho công chức chuyên trách công nghệ thông tin quản lý, sử dụng để thực hiện phân quyền theo quyết định của Giám đốc Sở.

Điều 9. Trách nhiệm cá nhân khi tham gia sử dụng hệ thống thông tin

1. Đối với việc kết nối và truy cập mạng Internet

Việc kết nối mạng Internet với hệ thống thông tin là để phục vụ công việc chuyên môn, nghiêm cấm các hành vi sau đây trong quá trình sử dụng kết nối mạng Internet:

a) Chia sẻ và phát tán các nội dung trái quy định pháp luật.

b) Sử dụng kết nối Internet để tải về hoặc sử dụng phim, nhạc, trò chơi trực tuyến trong giờ làm việc hành chính.

c) Tự ý cho người ngoài cơ quan sử dụng kết nối mạng Internet để thực hiện các mục đích ngoài công việc chuyên môn khi chưa được Giám đốc Sở cho phép.

d) Sử dụng kết nối mạng Internet để soạn thảo các văn bản, tài liệu "Mật" hoặc văn bản, tài liệu thuộc danh mục hạn chế sử dụng theo quy định pháp luật.

2. Đối với việc sử dụng máy tính để kết nối hệ thống thông tin

Máy tính do cơ quan trang bị là phương tiện để phục vụ công việc chuyên môn, được quản lý theo các quy định của pháp luật về quản lý tài sản nhà nước. Các hành vi sau đây phải thông báo cho công chức chuyên trách công nghệ thông tin biết và phải có sự đồng ý của Giám đốc Sở trước khi tiến hành:

a) Thay đổi cấu hình máy tính.

b) Kết nối máy tính với các mạng thông tin khác ngoài cơ quan.

c) Cài đặt các phần mềm khác với quy định của cơ quan.

d) Kết nối máy tính thuộc sở hữu riêng của cá nhân vào hệ thống thông tin.

3. Đối với việc quản lý, sử dụng tài khoản hệ thống thông tin

a) Cá nhân được cấp hoặc giao quản lý, sử dụng tài khoản hệ thống thông tin phải đặt mật khẩu theo các yêu cầu sau:

- Có chứa cả các ký tự chữ in và chữ thường.

- Có chứa ký tự số, các ký tự dấu câu hoặc các ký tự đặc biệt.

- Có ít nhất 08 ký tự đối với tài khoản người dùng, ít nhất 15 ký tự đối với tài khoản quản trị hệ thống.

- Không phải là một từ hoàn chỉnh trong các ngôn ngữ thông dụng (Tiếng Việt, Tiếng Anh, Tiếng Pháp,...).

- Không phải là một dãy ký tự lặp lại có quy luật.

- Không dựa vào thông tin cá nhân (ngày sinh, số điện thoại,...), tên người, tên địa danh, tên cơ quan hoặc các tên gọi khác.

b) Các hành vi sau đây bị nghiêm cấm khi sử dụng tài khoản hệ thống thông tin:

- Dùng chung một mật khẩu cho nhiều tài khoản hệ thống thông tin.

- Dùng mật khẩu tài khoản hệ thống thông tin cho các tài khoản khác của cá nhân như gmail, yahoo,...

- Cho cá nhân khác biết mật khẩu (trừ trường hợp Giám đốc Sở yêu cầu).

- Dùng chức năng ghi nhớ mật khẩu của các ứng dụng trên máy tính dùng chung như Google Chrome, FireFox,...

4. Phòng chống phần mềm có hại

a) Không truy cập và tải dữ liệu từ website, diễn đàn, mạng xã hội,... có nội dung trái quy định pháp luật.

b) Không mở các tài liệu, tập tin gửi kèm khi nhận thư điện tử có địa chỉ lạ hoặc không đáng tin cậy.

c) Không tự ý chia sẻ quyền truy cập ổ đĩa máy tính qua mạng nội bộ (trừ trường hợp có sự đồng ý của Giám đốc Sở).

d) Quét virus và các phần mềm có hại trên các phương tiện lưu trữ gắn ngoài như USB, thẻ nhớ, đĩa cứng gắn ngoài,...trước khi sử dụng.

5. Đối với việc sử dụng thư điện tử công vụ

a) Phải kịp thời thông báo cho công chức chuyên trách công nghệ thông tin hoặc báo cáo Giám đốc Sở khi nhận được thư điện tử có dấu hiệu lạ, có thể vi phạm pháp luật hoặc có khả năng gây ảnh hưởng đến công việc, uy tín, danh dự, tài sản của bản thân, cơ quan hoặc tổ chức, cá nhân khác.

b) Nghiêm cấm các hành vi sau đây:

- Sử dụng thư điện tử công vụ cho các mục đích ngoài công việc chuyên môn hoặc phát tán các nội dung trái quy định pháp luật.

- Sử dụng thư điện tử công vụ nhằm quấy rối hay làm gián đoạn công việc của tổ chức, cá nhân khác.

- Đặt chế độ chuyển thư tự động từ tài khoản thư điện tử công vụ tới tài khoản thư điện tử không chính thức như gmail, yahoo,...

- Phát tán phần mềm có hại hoặc thư rác qua hệ thống thư điện tử công vụ.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 10. Trách nhiệm công chức chuyên trách công nghệ thông tin

1. Sử dụng các chức năng của công cụ tường lửa (nếu có) để cấm truy cập cổng/trang thông tin điện tử, diễn đàn, mạng xã hội, địa chỉ trực tuyến hoặc mạng thông tin theo quy định pháp luật.

2. Tham mưu Giám đốc Sở quy định các chương trình, phần mềm được phép cài đặt trên máy tính chỉ nhằm mục đích phục vụ cho công tác quản lý nhà nước. Cài đặt phần mềm diệt virus và hệ điều hành có bản quyền, thường xuyên cập nhật các bản vá bảo mật để đảm bảo an toàn cho hệ thống thông tin.

3. Cấu hình, phân quyền trên máy tính dùng chung để mỗi cá nhân chỉ truy cập được thư mục dữ liệu của mình, không truy cập được thư mục dữ liệu của các cá nhân khác.

4. Các tài khoản quản trị hệ thống thông tin (tài khoản quản trị máy chủ, thiết bị mạng, phần mềm ứng dụng và cơ sở dữ liệu) phải thay đổi mật khẩu định kỳ, ít nhất 03 tháng 1 lần.

5. Chủ động phối hợp với Sở Thông tin và Truyền thông khóa hoặc thu hồi tài khoản thư điện tử công vụ nếu người sử dụng không tuân thủ các quy định của pháp luật hoặc việc sử dụng đã làm tổn hại nghiêm trọng đến công việc và uy tín của cơ quan.

6. Chỉ cho phép các máy tính và thiết bị được trang bị cơ chế bảo mật (cơ chế định danh thiết bị và trang bị phần mềm chống các phần mềm có hại) thực hiện kết nối từ xa vào hệ thống thông tin.

Điều 11. Trách nhiệm Văn phòng Sở

1. Nâng cấp, bảo dưỡng hệ thống máy chủ, thiết bị mạng và thiết bị bảo vệ mạng; đào tạo người sử dụng để thực hiện hiệu quả công tác đảm bảo an toàn thông tin số.

2. Phổ biến các quy định về an toàn thông tin số đến cán bộ, công chức, người lao động; trang bị kiến thức bảo mật cho người sử dụng theo hướng dẫn của Sở Thông tin và Truyền thông.

3. Khi xảy ra sự cố mất an toàn thông tin số, phải áp dụng mọi biện pháp để khắc phục và hạn chế thiệt hại, lập biên bản và báo cáo bằng văn bản cho cơ quan cấp trên quản lý trực tiếp. Trường hợp sự cố nghiêm trọng vượt quá khả năng khắc phục, phải báo cáo ngay cho cơ quan cấp trên quản lý trực tiếp và thông báo cho Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ.

4. Báo cáo tổng hợp tình hình thực hiện công tác đảm bảo an toàn thông tin số theo định kỳ và theo yêu cầu đột xuất của cơ quan có thẩm quyền.

Điều 12. Điều khoản thực hiện

Văn phòng Sở chủ trì, phối hợp các phòng, đơn vị thực hiện nghiêm túc quy định này./.

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ CÔNG THƯƠNG
TỈNH KHÁNH HÒA

Lê Thu Hải