UBND TỈNH QUẢNG TRỊ
SỞ CÔNG THƯƠNG

Số: 124 /QĐ-SCT

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

Quảng Trị, ngày 12 tháng 12 năm 2018

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 Công Thương Quảng Trị

GIÁM ĐỐC SỞ CÔNG THƯƠNG QUẢNG TRỊ

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 Nghị định 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 Quyết định số 35/2016/QĐ-UBND ngày 29/8/2016 của UBND tỉnh Quảng Trị Ban hành 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 nhà nước tỉnh Quảng Trị;

Căn cứ Quyết định số 34/2016/QĐ-UBND ngày 29/8/2016 của UBND tỉnh Quảng Trị về việc Ban hành Quy định, chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Công Thương Quảng Trị;

Theo đề nghị của Chánh Văn phòng Sở,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Sở Công Thương Quảng Trị.

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

Chánh Văn phòng, Chánh Thanh tra, Trưởng các phòng chuyên môn thuộc Sở, Thủ trưởng các đơn vị liên quan và toàn thể cán bộ, công chức và người lao động thuộc Sở chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như điều 3;
- Sở TTTT;
- GĐ, các PGĐ Sở;
- Lưu VT,VP.

GIÁM ĐỐC

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

Lê Quang Vĩnh

UBND TỈNH QUẢNG TRỊ
SỞ CÔNG THƯƠNG

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

QUY CHẾ
Đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Sở Công Thương Quảng Trị

(Ban hành kèm theo Quyết định số: 124/QĐ-SCT ngày 12/12/2018 của Sở Công Thương Quảng Trị)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về việc đảm bảo bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin (sau đây gọi tắt là CNTT) của Sở Công Thương Quảng Trị.

Điều 2. Đối tượng áp dụng

Quy chế này được áp dụng với toàn thể cán bộ công chức và người lao động thuộc Sở Công Thương.

Điều 3. Mục đích, nguyên tắc đảm bảo an toàn, an ninh mạng

1. Việc áp dụng quy chế này nhằm giảm thiểu được các nguy cơ mất an toàn thông tin và đảm bảo an ninh thông tin trong hoạt động ứng dụng CNTT của Sở Công Thương.

2. Các hoạt động ứng dụng CNTT phải tuân theo nguyên tắc đảm bảo an toàn thông tin được quy định tại Điều 4, Luật An toàn thông tin mạng; Điều 41, Nghị định 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về ứng dụng CNTT trong hoạt động của cơ quan nhà nước.

Điều 4. 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. *An ninh thông tin:* Là sự bảo đảm thông tin, hệ thống thông tin được phục vụ liên tục, tránh bị gián đoạn, ngăn chặn các truy cập trái phép làm sửa đổi, phá hoại hoặc rò rỉ thông tin.

3. *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 nhập, xử lý, lưu trữ và trao đổi thông tin.

4. *Hệ thống mạng LAN:* Là hệ thống mạng nội bộ dùng để kết nối các máy

tính trong một phạm vi nhỏ *(nhà ở, phòng làm việc, trường học,...)*. Các máy tính trong mạng LAN có thể chia sẻ tài nguyên với nhau, mà điển hình là chia sẻ tập tin, máy in, máy quét và một số thiết bị khác.

5. *Địa chỉ IP:* Là một địa chỉ đơn nhất mà những thiết bị điện tử hiện nay đang sử dụng để nhận diện và liên lạc với nhau trên mạng máy tính bằng cách sử dụng giao thức Internet.

6. *Thiết bị CNTT:* Là toàn bộ các máy móc, thiết bị có liên quan đến CNTT như: Máy vi tính (PC, laptop, server), máy in, máy scan, máy chiếu, thiết bị lưu trữ, camera số, thiết bị chuyển mạch (hub, switch), modem, firewall, hệ thống cáp mạng…

7. *Thiết bị lưu trữ ngoài:* Là các ổ cứng di động, USB, đĩa CD, DVD,…

8. *Tính sẵn sàng:* Là bảo đảm những người được cấp quyền có thể truy cập thông tin và các tài liệu có liên quan ngày khi có nhu cầu.

9. *Tính bảo mật:* Là bảo đảm những người được phép mới có thể truy cập thông tin.

10. *Tính toàn vẹn:* Là bảo vệ tính chính xác và đầy đủ của thông tin và các phương pháp xử lý.

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

12. *Tường lửa (Firewall):* Là rào chắn (phần cứng, phần mềm) được lập ra nhằm kiểm soát người dùng mạng Internet truy nhập vào các thông tin không mong muốn và người dùng từ bên ngoài truy nhập trái phép thông tin trong mạng nội bộ.

13. *Môi trường mạng:* Là môi trường trong đó thông tin được cung cấp, truyền đưa, thu nhập, xử lý, lưu trữ và trao đổi thông qua cơ sở hạ tầng thông tin.

14. *Bí mật nhà nước:* Là những tin về cụ, việc, tài liệu, vật, địa điểm, thời gian, lời nói có nội dung quan trong thuộc lĩnh vực chính trị, quốc phòng, an ninh, đối ngoại, kinh tế, khoa học, công nghệ, các lĩnh vực khác mà Nhà nước không công bố hoặc chưa công bố và nếu tiết lộ thì gây nguy hại cho nước Công hòa xã hội chủ nghĩa Việt Nam.

15. *Hacker*: Là người có thể viết hay chỉnh sửa phần mềm, phần cứng máy tính bao gồm lập trình, quản trị và bảo mật. Những người này hiểu rõ hoạt động của hệ thống máy tính, mạng máy tính và dùng kiến thức của bản thân để làm thay đổi, chỉnh sửa nó với nhiều mục đích tốt xấu khác nhau.

16. *Phần mềm độc hại:* là phần mềm có tính năng gây hại, gây ra hoạt động không bình thường cho một phần hay 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.

Chương II
QUẢN LÝ, SỬ DỤNG THIẾT BỊ CNTT

Điều 5. Sử dụng thiết bị CNTT

1. Thiết bị CNTT được trang bị tại các phòng, cá nhân thuộc Sở là tài sản của Nhà nước, được quản lý, sử dụng theo quy định của Sở.

2. Các phòng, cán bộ, công chức và người lao động thuộc Sở có trách nhiệm quản lý trang thiết bị CNTT được giao, quản lý dữ liệu trên máy tính của mình được cấp sử dụng, tự quyết định việc chia sẽ tài nguyên với các máy tính khác theo đúng quy định.

3. Không được tự ý thay thế các linh kiện của thiết bị CNTT.

Điều 6. Sửa chữa thiết bị CNTT

1. Trong quá trình sử dụng các thiết bị CNTT, nếu có sự cố xảy ra, cán bộ, công chức và người lao động thuộc lập phiếu đề xuất yêu cầu sửa chữa và có xác nhận của Lãnh đạo phòng, Sở.

2. Văn phòng Sở có trách nhiệm liên hệ kỹ thuật kiểm tra và thực hiện sửa chữa, thay thế theo đề xuất (sửa chữa nhỏ: đổ mực, cài máy…). Đối với các sự cố, hư hỏng lớn, nếu đưa thiết bị ra bên ngoài phải được sự đồng ý của lãnh đạo và có biên bản bàn giao nhận, nếu các sự cố hư hỏng buộc phải thay thế thiết bị phải có báo giá cụ thể của các đơn vị cung cấp.

Điều 7. Hệ thống mạng LAN của Sở

1. Mạng LAN Sở Công Thương là mạng cục bộ bao gồm hệ thống mạng dây, các thiết bị mạng, các thiết bị tin học nối lại với nhau thành một hệ thống mạng cục bộ cho phép kết nối với nhau để cùng làm việc và chia sẽ dữ liệu. Kết nối này được thực hiện thông qua sợi cáp LAN hay Wifi (không dây).

2. Mạng LAN của Sở Công Thương là mạng vật lý riêng, có địa chỉ và các tham số mạng, được sử dụng để phục phụ công tác quản lý, chỉ đạo điều hành, phối hợp công tác trong nội bộ cơ quan.

3. Văn phòng Sở trực tiếp quản lý, vận hành hệ thống mạng máy tính của cơ quan Sở hoạt động thông suốt 24h/24h.

Chương III
ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 8. 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 phù hợp.

2. Quản lý hệ thống mạng không dây: thường xuyên 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 thường xuyên kiểm tra 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 đối với cán bộ, công chức, viên chức đã chuyển công tác, chấm dứt hợp đồng lao động.

4. Chống mã độc, virus: Lựa chọn, triển khai các phần mềm chống virus, thư rác trên máy tính, các thiết bị di động trong mạng và những hệ thống thông tin xung yếu như: trang 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. 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, thiết lập chế độ quét thường xuyên ít nhất là hằng tuần.

5. Tổ chức quản lý tài nguyên: Kiểm tra, giám sát chức năng chia sẽ thông tin (Network File and Folder Sharing). Khuyến cáo người sử dụng cân nhắc việc chia sẽ tài nguyên cục bộ trên máy đang sử dụng, tuyệt đối không được chia sẽ toàn bộ ổ cứng. Khi thực hiện việc chia sẽ tài nguyên trên máy chủ hoặc trên máy cục bộ nên sử dụng mật khẩu để bảo vệ thông tin.

6. Các biện pháp kỹ thuật bảo đảm an toàn cho Trang thông tin điện tử (gọi tắt là trang web): Phối hợp với Trung tâm tin học tỉnh để có các phương án sao lưu, bảo mật các dịch vụ liên quan trên Trang thông tin điện tử của Sở.

Điều 9. Quy định về bảo mật và an toàn dữ liệu

1. Quy định về soạn thảo, in ấn, phát hành và sao chụp tài liệu mật:

a) Không được sử dụng máy tính có kết nối internet để soạn thảo văn bản, chuyển giao, lưu trữ thông tin có nội dung thuộc bí mật nhà nước theo danh mục quy định; cung cấp tin, tài liệu và đưa thông bí mật nhà nước lên Cổng/Trang thông tin điện tử.

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

c) Khi sửa chữa, khắc phục các sự cố máy tính dùng soạn thảo văn bản mật phải báo cáo cho cơ quan có thẩm quyền. Không được cho phép các công ty tư nhân hoặc người không có trách nhiệm trực tiếp sửa chữa, xử lý, khắc phục sự cố.

d) Trước khi thanh lý các máy tính tại Sở, cán bộ phụ trách CNTT của Sở phải dùng các biện pháp kỹ thuật xóa bỏ vĩnh viễn dữ liệu trong ổ cứng của máy tính.

2. Nghiêm cấm hành vi để lộ thông tin (tên truy cập, mật khẩu, địa chỉ IP liên quan đến Sở) cho các đối tượng không liên quan bên ngoài.

3. Người sử dụng tự chịu trách nhiệm việc bảo vệ dữ liệu máy tính được giao sử dụng, kể cả tài nguyên được chia sẽ. Không được xóa dữ liệu đang

được chia sẽ trong hệ thống mạng. Có trách nhiệm tự lưu trữ dự phòng dữ liệu để đảm bảo an toàn dữ liệu khi có sự cố xảy ra.

4. Đối với một số máy tính có dữ liệu quan trọng như máy Văn thư, Kế toán cần có thêm thiết bị lưu trữ ngoài để lưu trữ dữ liệu dự phòng.

Điều 10. Quản lý truy cập

1. Việc truy cập vào hệ thống thông tin liên quan đến hoạt động của Sở phải xuất phát từ yêu cầu phục vụ công tác quản lý, điều hành, sử dụng chung của cơ quan.

2. Mỗi cán bộ, công chức, người lao động cơ quan Sở chỉ được phép truy cập các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình và tự bảo mật tài khoản truy cập của mình.

3. Trường hợp có sự thay đổi về vị trí việc làm, chuyển công tác, nghỉ hưu… cần có các biện pháp quản lý chặt chẽ trong việc quản lý truy cập vào hệ thống thông tin của Sở.

4. Cá nhân truy cập từ xa vào các ứng dụng thông tin của Sở có trách nhiệm bảo mật thông tin. Tránh các trường hợp đăng nhập các thiết bị bên ngoài bị lưu lại tài khoản và mật khẩu đăng nhập. Nghiêm cấm việc cung cấp, để lộ lọt thông tin nội bộ khi chưa có sự chỉ đạo, cho phép.

Điều 11. Những hành vi bị nghiêm cấm

1. Không được lợi dụng việc sử dụng mạng internet nhằm mục đích: Chống lại Nhà nước, gây hại đến an ninh quốc gia, trật tự an toàn xã hội; kích động bạo lực, đồi trụy, tệ nạn xã hội, mê tín di đoan, phá hoại thuần phong mỹ tục của đơn vị.

2. Không được tiết lộ bí mật nhà nước và các bí mật khác đã được pháp luật quy định.

3. Không được đưa hoặc thu thập thông tin xuyên tạc, vu khống, xúc phạm uy tín của cơ quan, danh dự nhân phẩm của cán bộ, công chức, người lao động hoặc công dân.

4. Không được gây rối, phá hoại hệ thống thiết bị công nghệ thông tin của Sở.

5. Không được chơi các trò chơi trực tuyến, các chương có nội dung xấu, không lành mạnh trong giờ làm việc.

6. Không được cài đặt các phần mềm không rõ nguồn gốc, không có bản quyền nhằm tránh những nguy cơ bị đánh cắp thông tin cũng như virus phá hoại.

7. Không đươc kết nối máy tính với các thiết bị ngoại vi (ổ cứng di động, USB…) khi không có chương trình diệt virus đảm bảo.

8. Không được truy cập, sửa đổi, xóa bỏ những nội dung thông tin của cơ quan, cá nhân khác khi không được sự cho phép hoặc cấp quyền.

Chương IV

TRÁCH NHIỆM ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 12. Trách nhiệm của các phòng thuộc Sở

1. Tăng cường công tác tuyên truyền, nâng cao nhận thức cho cán bộ, công chức về nguy cơ mất an toàn, an ninh thông tin. Phổ biến các nội dung, hướng dẫn theo quy định tại Quy chế này.

2. Tăng cường ứng dụng ký số các loại văn bản điện tử theo quy định nhằm đảm bảo an toàn trong việc trao đổi văn bản điện tử qua môi trường mạng; hệ thống xác thực tài khoản và mã hóa dự liệu…

3. Tăng cường sử dụng thư điện tử công vụ để gửi các văn bản, trao đổi công việc trong các cơ quan nhà nước, tuyệt đối không sử dụng các hộp thư điện tử miễn phí (Gmail, yahoo...) nhằm bảo đảm bảo mật, an toàn thông tin trên môi trường mạng.

4. Đối với các tài khoản đăng nhập vào các hệ thống thông tin, quản lý của Sở, địa chị email công vụ, email, facebook cá nhân..., cần thay đổi mật khẩu theo định kỳ và mật khẩu phải có độ phức tạp cao; hạn chế việc sử dụng email miễn phí, trong trường hợp có đính kèm các tài liệu quan trọng gửi qua email phải đặt mật khẩu để đảm bảo an toàn.

5. Thường xuyên kiểm tra, cập nhật các bản vá lỗ hỏng bảo mật từ các nhà cung cấp sản phẩm, dịch vụ;

Điều 13. Trách nhiệm của Văn phòng Sở

1. Tham mưu cử cán bộ tham gia các lớp bồi dưỡng, đào tạo về CNTT để trang bị các kiến thức về an toàn, an ninh thông tin.

2. Phân bổ kinh phí chi thường xuyên cần thiết cho các hoạt động liên quan đến việc ứng dụng CNTT trong hoạt động của cơ quan Sở.

3. Tham mưu chuyên môn và vận hành an toàn hệ thống thông tin của Sở, triển khai các biện pháp bảo đảm an toàn, an ninh thông tin cho tất cả cán bộ, công chức trong cơ quan Sở.

4. Nắm vững và thực hiện nghiêm túc Pháp lệnh bảo vệ bí mật Nhà nước; Thường xuyên tự cập nhật các kiến thức về an toàn, an ninh thông tin, nguy cơ tiềm ẩn có thể gây mất mát thông tin và các biện pháp phòng tránh.

5. Phối hợp chặt chẽ với cơ quan, đơn vị liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn, an ninh thông tin.

Điều 14. Trách nhiệm của cán bộ, công chức và người lao động thuộc Sở

1. Thường xuyên cập nhật những văn bản, hướng dẫn về an toàn, an ninh thông tin. Nghiêm chỉnh chấp hành các quy chế nội bộ, quy định 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 Sở.

2. Hạn chế việc sử dụng chức năng chia sẽ tài nguyên (sharing), khi sử dụng chức năng này cần bật thuộc tính bảo mật bằng mật khẩu và thực hiện việc thu hồi chức năng này khi đã sử dụng xong.

3. Các máy tính khi không sử dụng trong thời gian dài (quá 2 giờ làm việc) cần tắt máy hoặc ngưng kết nối mạng, để tránh bị các hacker lợi dụng, sử dụng chức năng điều khiển từ xa dùng máy tính của mình tấn công vào các hệ thống thông tin khác.

4. Sử dụng chức năng mã hóa ở mức hệ điều hành bảo đảm các dữ liệu nhạy cảm như tài khoản, mật khẩu, các tập tin văn bản... được mã hóa trước khi truyền trên môi trường mạng. Các tập tin gửi đính kèm bởi thư điện tử hoặc được tải xuống từ Internet hay các thiết bị lưu trữ gắn vào hệ thống cần được kiểm tra để phòng chống lây nhiễm virus hoặc phần mềm gián điệp gây mất mát thông tin.

5. Khi phát hiện có sự cố mất an toàn an ninh thông tin cần phải báo ngay với cán bộ phụ trách CNTT và Văn phòng Sở để kịp thời xử lý.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 15. Trách nhiệm thi hành

1. Văn phòng Sở có trách nhiệm triển khai hướng dẫn thực hiện các nội dung của Quy chế này.

2. Các phòng và toàn thể cán bộ, công chức và người lao động thuộc Sở có trách nhiệm thi hành Quy chế này.

Trong quá trình thực hiện nếu có phát sinh khó khăn, vướng mắc đề nghị kịp thời phản ánh về Văn phòng Sở để tổng hợp báo cáo Lãnh đạo Sở xem xét, sửa đổi, bổ sung Quy chế cho phù hợp./.

GIÁM ĐỐC

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

Lê Quang Vĩnh