BỘ TÀI CHÍNH	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
	Độc lập - Tự do – Hạnh phúc
Số: 2615/QĐ-BTC	

Hà Nội, ngày 19 tháng 10 năm 2012

QUYẾT ĐỊNH
Ban hành Quy định về việc đảm bảo an toàn thông tin trên môi trường máy tính và mạng máy tính

BỘ TRƯỞNG BỘ TÀI CHÍNH

Căn cứ Nghị định số 118/2008/NĐ-CP ngày 27/11/2008 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Tài chính;

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về việc ứng dụng công nghệ thông tin trong hoạt động của cơ quan Nhà nước;

Căn cứ Nghị định số 33/2002/NĐ-CP ngày 28/3/2002 của Chính phủ về việc quy định chi tiết thi hành Pháp lệnh bảo vệ bí mật Nhà nước;

Căn cứ Quyết định số 196/2003/QĐ-BTC ngày 02/12/2003 của Bộ trưởng Bộ Tài chính về việc ban hành Quy chế bảo vệ bí mật nhà nước của ngành Tài chính;

Theo đề nghị của Cục trưởng Cục Tin học và Thống kê tài chính,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy định về việc đảm bảo an toàn thông tin trên môi trường máy tính và mạng máy tính.

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

Điều 3. Cục trưởng Cục Tin học và Thống kê tài chính, Chánh Văn phòng Bộ, Thủ trưởng các cơ quan hành chính, đơn vị sự nghiệp thuộc Bộ Tài chính, Sở Tài chính các tỉnh, thành phố trực thuộc Trung ương, Phòng Kế hoạch Tài chính thuộc Sở Tài chính các địa phương và các đơn vị, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Lãnh đạo Bộ;
- Các đơn vị thuộc Bộ;
- Sở Tài chính các tỉnh, thành phố trực thuộc TW;
- Lưu: VT, Cục THTK.(115)

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Phạm Sỹ Danh

BỘ TÀI CHÍNH

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

QUY ĐỊNH
Về việc đảm bảo an toàn thông tin
trên môi trường máy tính và mạng máy tính
(Ban hành kèm theo Quyết định số 2615/QĐ-BTC ngày 15 tháng 10 năm 2012 của Bộ trưởng Bộ Tài chính)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi và đối tượng áp dụng

1. Phạm vi áp dụng:

Quy định này bao gồm các điều kiện tối thiểu phải tuân thủ nhằm đảm bảo an toàn thông tin trên môi trường máy tính, mạng máy tính và các hệ thống có khả năng tiếp cận thông tin số của ngành Tài chính. Thông tin được đảm bảo an toàn bao gồm tất cả các loại thông tin của Bộ Tài chính và các đơn vị thuộc Bộ, thông tin tại các cơ quan tài chính địa phương thuộc lĩnh vực do Bộ Tài chính quản lý, thông tin do các cơ quan, tổ chức khác gửi đến Bộ Tài chính và các đơn vị thuộc Bộ.

2. Đối tượng áp dụng:

a) Các đơn vị thuộc Bộ Tài chính và cán bộ, công chức, viên chức, nhân viên của đơn vị: áp dụng đầy đủ Quy định này.

b) Các Sở Tài chính, Phòng Kế hoạch Tài chính và cán bộ, công chức, viên chức, nhân viên của đơn vị: áp dụng Quy định này cho các máy tính, mạng máy tính và ứng dụng phục vụ hoạt động chuyên môn của đơn vị thuộc lĩnh vực quản lý của Bộ Tài chính.

c) Cơ quan, tổ chức, cá nhân có hoạt động trao đổi thông tin với các đơn vị thuộc Bộ Tài chính (Đối tác tham gia tư vấn, xây dựng, triển khai, hỗ trợ, vận hành, thử nghiệm hệ thống công nghệ thông tin; Cơ quan, tổ chức, cá nhân có kết nối mạng để trao đổi thông tin với các đơn vị thuộc ngành Tài chính): áp dụng quy định trong hoạt động trao đổi thông tin với ngành Tài chính.

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. "Mạng nội bộ cơ quan Bộ Tài chính": hệ thống mạng máy tính tại trụ sở cơ quan Bộ Tài chính, phần mở rộng của mạng này tới trụ sở của các đơn vị thuộc Bộ đặt ngoài trụ sở cơ quan Bộ Tài chính và Đại diện Văn phòng Bộ Tài chính tại thành phố Hồ Chí Minh.

3. "Hạ tầng truyền thông thống nhất ngành Tài chính": hệ thống mạng diện rộng kết nối các mạng máy tính của các đơn vị thuộc ngành Tài chính.

4. "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 (~, !,...).

5. "Thuật toán mã hoá an toàn" là thuật toán mã hoá 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 hoá.

6. "Bí mật nhà nước": thông tin thuộc Danh mục Bí mật Nhà nước cấp độ tuyệt mật, tối mật, mật của ngành Tài chính theo quy định hiện hành và bí mật nhà nước của các cơ quan, đơn vị khác gửi đến Bộ Tài chính.

7. "Đơn vị": các đơn vị thuộc phạm vi áp dụng của quy định này.

8. "Đơn vị hệ thống thuộc Bộ": Tổng cục Thuế, Tổng cục Hải quan, Tổng cục Dự trữ Nhà nước, Kho bạc Nhà nước, Ủy ban Chứng khoán Nhà nước, Học viện Tài chính.

9. "Người dùng": cán bộ, công chức, viên chức, nhân viên hợp đồng của đơn vị 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. Đơn vị, 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 Bộ Tài chính và hướng dẫn của các cơ quan, đơn vị có thẩm quyền trong lĩnh vực đảm bảo an toàn thông tin.

3. Người dùng phải được tập huấn kiến thức chung về an toàn thông tin trên môi trường máy tính, mạng máy tính và kiến thức nâng cao về an toàn thông tin 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 Tài chính 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: Trung tâm dữ liệu, khu vực chứa 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. Đơn vị quản lý các vùng thiết bị trên phải có nội quy hoặc hướng dẫn làm việc trong các khu vực này.

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 không sử dụng tiếp cho công việc của đơn vị (thanh lý, cho, tặng) phải được xoá 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, máy quản trị và máy tính phục vụ công việc của người dùng tại đơn vị):

a) Máy tính làm việc chỉ được cài đặt phần mềm theo danh mục phần mềm do đơn vị quy định và do bộ phận công nghệ thông tin của đơn vị quản lý hoặc được cung cấp theo các chương trình ứng dụng công nghệ thông tin của Bộ Tài chính hoặc các cơ quan Nhà nước khác có thẩm quyền, 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 đơn vị chịu trách nhiệm cài đặt 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 đơn vị.

c) Người dùng phải thực hiện thao tác khoá 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 của đơn vị và các hệ thống mạng của ngành Tài chính.

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

1. Kết nối mạng diện rộng phải được thiết lập và vận hành theo Quy chế quản lý, vận hành và sử dụng hạ tầng truyền thông thống nhất ngành Tài chính ban hành tại Quyết định số 109/QĐ-BTC ngày 15/01/2009 của Bộ trưởng Bộ Tài chính và các văn bản sửa đổi, cập nhật quy chế này nếu có.

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

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

Mạng nội bộ cơ quan Bộ Tài chính và các đơn vị hệ thống thuộc Bộ tại cấp Trung ương phải phân chia tối thiểu thành các vùng mạng sau:

- Vùng mạng cho truy cập từ Internet (áp dụng đối với các đơn vị có cổng thông tin điện tử, dịch vụ công hoặc ứng dụng cung cấp ra Internet đặt tại đơn vị).

- Vùng mạng truy cập Internet (trung chuyển các yêu cầu truy cập Internet từ người dùng hoặc máy chủ);

- Vùng mạng máy chủ nội bộ;

- Vùng mạng quản trị hệ thống (các hoạt động quản trị hệ thống phải được thực hiện thông qua vùng mạng này);

- Vùng mạng người dùng, trong đó tách riêng vùng mạng cho kết nối có dây và không dây.

- Vùng mạng riêng cho khách (áp dụng đối với các đơn vị cho phép khách đến làm việc được truy cập hệ thống mạng của đơn vị để sử dụng Internet).

b) Vô hiệu hoá 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 Tài chính).

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 cơ quan Bộ Tài chính và các đơn vị hệ thống thuộc Bộ tại cấp Trung ương phải được giám sát bởi hệ thống phát hiện và phòng chống tấn công.

4. Hệ thống mạng không dây (nếu có) phải đáp ứng các điều kiện tối thiểu sau:

a) Thiết bị phần cứng phải có chứng nhận Wi-Fi (chứng nhận của Liên minh Wi-Fi (www.wi-fi.org) cho sản phẩm đạt tiêu chuẩn 802.11);

b) Áp dụng mã hoá dữ liệu truyền nhận sử dụng thuật toán mã hoá an toàn;

c) Người dùng không dây phải được cung cấp định danh duy nhất và xác thực qua kênh mã hoá.

d) Các điểm truy cập không dây 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 đơn vị phải được đảm bảo an toàn theo quy định tại Điều 5;

b) Kết nối truy cập từ xa phải sử dụng mã hoá 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. Đơn vị áp dụng các biện pháp cần thiết để đảm bảo an toàn thông tin trong hoạt động kết nối Internet của người dùng tại đơn vị, tối thiểu đáp ứng yêu cầu sau:

a) Có tường lửa kiểm soát truy cập Internet.

b) 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 Tài chính không được mở trang tin hoặc ứng dụng Internet ngay trên máy này hoặc chỉ được phép truy cập vào các trang tin trên Internet phục vụ công việc của đơn vị.

Cục Tin học và Thống kê Tài chính căn cứ các quy định của pháp luật và ý kiến của các đơn vị tại trụ sở Bộ Tài chính xác định và trình Bộ phê duyệt danh sách các loại dữ liệu và ứng dụng quan trọng trên hệ thống mạng nội bộ cơ quan Bộ Tài chính cần được bảo vệ trong kết nối Internet.

Đối với các đơn vị hệ thống thuộc Bộ và các Sở Tài chính, lãnh đạo đơn vị quyết định các loại dữ liệu và ứng dụng quan trọng của đơn vị cần bảo vệ trong kết nối Internet của người dùng.

d) Kết nối Internet cho máy tính làm việc của người dùng tại đơn vị bị thu hẹp phạm vi hoặc bị ngắt trong các trường hợp sau:

- Có công văn từ Bộ Tài chính yêu cầu thu hẹp phạm vi kết nối Internet hoặc ngắt kết nối Internet (áp dụng trong các trường hợp khẩn cấp).

- Lãnh đạo đơn vị quyết định phải hạn chế phạm vi kết nối hoặc ngắt hoàn toàn kết nối Internet máy tính làm việc của người dùng để đảm bảo an toàn cho hệ thống mạng của đơn vị và hạn chế các ảnh hưởng khác của Internet tới hoạt động của đơn vị.

đ) 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, dịch vụ công, 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 vào Internet.

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 do đơn vị phát triển hoặc thuê phát triển phải đáp ứng yêu cầu sau:

- Mã hoá thông tin bí mật hoặc nhạy cảm bằng thuật toán mã hoá 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 hoá, trong đó:

- Bí mật nhà nước của ngành Tài chính phải được mã hoá bằng giải pháp do Ban Cơ yếu Chính phủ cung cấp hoặc chấp nhận sử dụng trong ngành Tài chính; trường hợp chưa có hướng dẫn của Ban Cơ yếu Chính phủ thì phải được sự đồng ý của Bộ Tài chính và đảm bảo tuân thủ quy định của Nhà nước về cơ yếu.

- Áp dụng mã hoá kênh kết nối cho các hoạt động sau: quản trị hệ thống; đăng nhập mạng, ứng dụng; gửi nhận dữ liệu tự động giữa các máy chủ; nhập và biên tập dữ liệu; tra cứu dữ liệu mật, nhạy cảm.

- Khuyến khích áp dụng công nghệ chữ ký số để xác thực và bảo mật dữ liệu, đặc biệt trong trường hợp cần đảm bảo chống từ chối nguồn gốc dữ liệu.

- Văn bản điện tử có nội dung cần hạn chế tiếp cận nhưng không thuộc danh mục bí mật Nhà nước được sử dụng tính năng mã hoá (đặt mật khẩu) của các ứng dụng văn phòng (phần mềm soạn thảo, đọc văn bản, nén tệp), nhưng phải sử dụng thuật toán mã hoá an toàn.

2. Các cá nhân thực hiện soạn thảo, gửi, nhận dữ liệu có trách nhiệm xác định mức độ mật, nhạy cảm của dữ liệu để thực hiện phương thức bảo vệ dữ liệu phù hợp hoặc yêu cầu bộ phận công nghệ thông tin hướng dẫn, hỗ trợ phương thức bảo vệ trong trường hợp cần thiết.

3. Chỉ sử dụng hệ thống thư điện tử và các công cụ trao đổi thông tin do đơn vị quản lý trực tiếp, hoặc các cơ quan Nhà nước, các tổ chức có thẩm quyền cung cấp để trao đổi thông tin, tài liệu làm việc. Không sử dụng các phương tiện trao đổi thông tin công cộng trên Internet cho mục đích này.

Điều 10. Đảm bảo an toàn trong hoạt động trao đổi thông tin với các tổ chức, cá nhân ngoài ngành Tài chính

1. Các tổ chức và cá nhân thuộc phạm vi quy định tại điểm c khoản 2 Điều 1 phải có cam kết bảo mật thông tin của đơn vị và của ngành Tài chính trước khi bắt đầu thực hiện công việc theo hợp đồng, thoả thuận giữa hai bên.

2. Khi trao đổi các thông tin cần bảo mật của đơn vị và của ngành Tài chính giữa đối tác và đơn vị thông qua hệ thống mạng (thư điện tử, truyền tệp,...) phải thực hiện mã hoá trước khi trao đổi theo quy định tại Điều 9 của Quy định này.

4. Đối với trường hợp tổ chức, cá nhân bên ngoài có thiết lập kết nối mạng với đơn vị:

a) Phải thực hiện phân tích rủi ro về an toàn thông tin trước khi thực hiện kết nối mạng giữa đơn vị với tổ chức, cá nhân bên ngoài và có biện pháp kiểm soát các rủi ro này.

b) Hai bên phải thoả thuận bằng văn bản các điều kiện cụ thể mà tổ chức, cá nhân bên ngoài phải đáp ứng khi thiết lập kết nối mạng tới đơn vị và thực hiện kiểm tra định kỳ việc thực hiện thoả thuận này của tổ chức, cá nhân bên ngoài.

Điều kiện tổ chức, cá nhân bên ngoài phải đáp ứng tối thiểu bao gồm: phân đoạn mạng của tổ chức, cá nhân bên ngoài được sử dụng để kết nối với hệ thống mạng của đơn vị phải được kiểm soát bằng tường lửa, các máy tính trong phân đoạn mạng này phải được cập nhật bản vá hệ điều hành, mẫu phòng diệt virus, các tài khoản truy cập hệ thống tối thiểu phải áp dụng mật khẩu phức tạp, chỉ được kết nối Internet trong trường hợp kết nối này phục vụ cho công việc của đơn vị thuộc ngành Tài chính.

Điều 11. Sao lưu, dự phòng sự cố

1. Đơn vị phải có thiết bị và quy trình, nhân sự phục vụ công tác sao lưu dữ liệu phòng ngừa sự cố; định kỳ kiểm tra tác dụng của dữ liệu sao lưu và phục hồi thử hệ thống từ dữ liệu sao lưu.

2. Đối với các hệ thống mạng và ứng dụng quan trọng phải có biện pháp dự phòng về thiết bị, phần mềm, để đảm bảo sự hoạt động liên tục của hệ thống.

Điều 12. Tài khoản công nghệ thông tin

1. Tài khoản người dùng:

a). Mỗi người dùng khi sử dụng hệ thống mạng, ứng dụng của đơn vị và của ngành Tài chính phải được cấp tài khoản truy cập với định danh duy nhất gắn với người dùng đó. Trường hợp sử dụng tài khoản dùng chung cho một nhóm người hay một đơn vị phải có cơ chế xác định các cá nhân có trách nhiệm quản lý tài khoản.

b) Tài khoản truy cập mạng của người sử dụng không được có quyền quản trị trên máy tính nối mạng. Tài khoản quản trị máy tính chỉ được sử dụng trong trường hợp cài đặt phần mềm trên máy tính. Tài khoản quản trị máy tính để bàn phải do bộ phận công nghệ thông tin của đơn vị nắm giữ. Đối với máy tính xách tay, người dùng phải được hướng dẫn sử dụng đúng cách tài khoản quản trị máy tính và có trách nhiệm thực hiện theo đúng hướng dẫn.

c) Các quyết định, thông báo về việc người dùng điều chuyển công tác, thôi việc hoặc nghỉ việc phải được đồng thời chuyển cho bộ phận quản

lý tài khoản công nghệ thông tin để thực hiện điều chỉnh, thu hồi, hủy bỏ các quyền sử dụng của người dùng đối với hệ thống mạng và ứng dụng của đơn vị và của ngành Tài chính.

2. Tài khoản quản trị hệ thống (thiết bị, mạng, ứng dụng, cơ sở dữ liệu) phải tách biệt với tài khoản truy cập mạng, ứng dụng với tư cách người dùng thông thường. Tài khoản quản trị hệ thống phải được giao đích danh cá nhân làm công tác quản trị hệ thống. Nghiêm cấm dùng chung tài khoản quản trị.

3. Phương tiện xác thực tài khoản:

a) Mật khẩu phức tạp phải được áp dụng cho tất cả các tài khoản truy cập, sử dụng, quản trị hệ thống mạng, ứng dụng trên hệ thống mạng máy tính nội bộ của đơn vị và của ngành Tài chính.

b) Thực hiện đổi mật khẩu định kỳ, tối thiểu 3 tháng một lần đối với tài khoản của người dùng và 2 tháng một lần đối với tài khoản quản trị hệ thống.

c) Người dùng, người làm công tác quản trị hệ thống có trách nhiệm bảo vệ thông tin tài khoản được cấp, không tiết lộ mật khẩu hoặc đưa cho người khác phương tiện xác thực tài khoản của mình ngoại trừ các trường hợp: cần xử lý công việc khẩn cấp của đơn vị; cần cung cấp, bàn giao cho đơn vị các thông tin, tài liệu do cá nhân quản lý. Chủ tài khoản phải đổi mật khẩu ngay sau khi kết thúc xử lý các việc này.

Điều 13. Đảm bảo an toàn trong công tác quản trị hệ thống

1. Máy tính dùng để quản trị hệ thống chỉ được cài đặt các phần mềm cần thiết cho hoạt động quản trị hệ thống, đặt trong vùng mạng phục vụ công tác quản trị hệ thống và chỉ được cấp quyền truy cập cho các cá nhân được giao trách nhiệm quản trị hệ thống.

2. Thay đổi tên tài khoản và mật khẩu mặc định của quản trị hệ thống được cung cấp khi hệ thống được thiết lập.

3. Sử dụng kênh trao đổi thông tin an toàn (có mã hoá) cho truy cập quản trị hệ thống.

Điều 14. Quản lý an toàn thông tin

1. Đơn vị phải phân công nhân sự quản lý an toàn thông tin trên môi trường máy tính và mạng máy tính (bao gồm công tác giám sát, kiểm tra việc thực hiện quy định này tại đơn vị).

2. Đơn vị phải ban hành quy trình cụ thể về việc phát hiện, báo cáo, xử lý và quản lý hoạt động khắc phục các sự cố liên quan đến an toàn thông tin tại đơn vị.

3. Các hệ thống an ninh mạng (cập nhật bản vá hệ điều hành, phòng diệt virus máy tính, tường lửa, phát hiện và phòng chống tấn công,...) phải được giám sát thường xuyên để đảm bảo tác dụng của hệ thống, đồng thời phát hiện và xử lý sớm các vấn đề về an toàn thông tin. Thực hiện kết xuất định kỳ hàng tháng hoặc hàng quý các báo cáo từ hệ thống an ninh mạng để theo dõi, đánh giá các vấn đề của hệ thống.

4. Người dùng phải được tập huấn kiến thức về an toàn thông tin phù hợp phạm vi công việc và mức độ tham gia sử dụng máy tính; được bộ phận công nghệ thông tin của đơn vị hướng dẫn, hỗ trợ, cung cấp các công cụ cần thiết để thực hiện trách nhiệm đảm bảo an toàn thông tin theo quy định.

Chương III
TRÁCH NHIỆM CỦA ĐƠN VỊ, CÁ NHÂN

Điều 15. Trách nhiệm của các đơn vị

1. Cục Tin học và Thống kê tài chính:

a) Tổ chức phổ biến và triển khai thực hiện Quy định này tại cơ quan Bộ Tài chính và các đơn vị có kết nối vào mạng nội bộ cơ quan Bộ Tài chính.

b) Trình Bộ phê duyệt và tổ chức triển khai kế hoạch ứng phó trong tình huống khẩn cấp (phát hiện có tấn công ăn cắp bí mật nhà nước của ngành Tài chính qua đường mạng, các hệ thống thông tin quan trọng của ngành Tài chính bị chiếm quyền điều khiển...).

c) Hướng dẫn, kiểm tra việc thực hiện Quy định này của các Đơn vị hệ thống thuộc Bộ, các Sở Tài chính, các đơn vị có kết nối trao đổi thông tin với mạng nội bộ cơ quan Bộ Tài chính.

d) Hướng dẫn, kiểm tra các đơn vị thuộc Bộ Tài chính về việc thực hiện các yêu cầu của các cơ quan Nhà nước có thẩm quyền về đảm bảo an toàn thông tin trên môi trường máy tính và mạng máy tính.

đ) Tổng hợp, báo cáo Bộ theo định kỳ hàng quý về công tác đảm bảo an toàn thông tin của toàn ngành Tài chính theo các nội dung của Quy định này và các vấn đề về an toàn thông tin trên môi trường máy tính và mạng máy tính phát sinh trong kỳ báo cáo.

e) Trình Bộ sửa đổi, bổ sung Quy định này để phù hợp với tình hình và điều kiện thực tế.

2. Các đơn vị hệ thống thuộc Bộ Tài chính, Sở Tài chính:

a) Tổ chức triển khai thực hiện Quy định này tại đơn vị.

b) Triển khai hoạt động ứng phó khẩn cấp theo kế hoạch được Bộ phê duyệt và hướng dẫn của Cục Tin học và Thống kê Tài chính.

c) Các đơn vị hệ thống thuộc Bộ Tài chính hướng dẫn, kiểm tra việc thực hiện quy định của các đơn vị trực thuộc. Sở Tài chính hướng dẫn, kiểm tra việc thực hiện quy định của các Phòng Kế hoạch Tài chính trên cùng địa bàn tỉnh, thành phố.

d) Thực hiện các yêu cầu, hướng dẫn về an toàn thông tin trên môi trường máy tính và mạng máy tính của các cơ quan Nhà nước có thẩm quyền và của Cục Tin học và Thống kê Tài chính.

đ) Báo cáo Bộ (qua Cục Tin học và Thống kê Tài chính) theo định kỳ hàng quý tình hình công tác đảm bảo an toàn thông tin của đơn vị theo các nội dung của Quy định này và các vấn đề về an toàn thông tin trên môi trường máy tính và mạng máy tính phát sinh trong kỳ báo cáo.

e) Phản ánh các vướng mắc, đề xuất sửa đổi, bổ sung Quy định này trong quá trình thực hiện tới Cục Tin học và Thống kê Tài chính.

3. Các đơn vị tham gia sử dụng hệ thống mạng nội bộ cơ quan Bộ Tài chính

a) Phối hợp với Cục Tin học và Thống kê Tài chính trong việc triển khai, thực hiện quy định áp dụng cho đối tượng người dùng tại đơn vị.

b) Phối hợp với Cục Tin học và Thống kê Tài chính triển khai kế hoạch ứng phó tấn công khẩn cấp về các nội dung liên quan tới đơn vị.

c) Phản ánh nhu cầu, vướng mắc trong quá trình triển khai, thực hiện đảm bảo an ninh thông tin tại đơn vị tới Cục Tin học và Thống kê tài chính.

Điều 16. Trách nhiệm của cá nhân

1. Thủ trưởng đơn vị thuộc đối tượng áp dụng của Quy định này có trách nhiệm phổ biến tới từng cán bộ, công chức, viên chức, nhân viên của đơn vị; thường xuyên kiểm tra việc thực hiện Quy định này tại đơn vị, định kỳ hàng quý báo cáo Bộ (qua Cục Tin học và Thống kê Tài chính) chịu trách nhiệm trước pháp luật và Lãnh đạo Bộ Tài chính về các vi phạm, thất thoát thông tin, dữ liệu mật thuộc phạm vi quản lý của đơn vị do không tổ chức, chỉ đạo, kiểm tra sát sao cán bộ của đơn vị thực hiện đúng quy định.

2. Cán bộ, công chức, viên chức, nhân viên của Bộ Tài chính, các đơn vị thuộc Bộ và các đơn vị khác thuộc đối tượng áp dụng của quy định này chịu trách nhiệm trước pháp luật và Lãnh đạo đơn vị về các vi phạm, thất thoát dữ liệu mật của ngành Tài chính do không tuân thủ quy định./.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Phạm Sỹ Danh