BỘ TÀI CHÍNH	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
	Độc lập - Tự do – Hạnh phúc
Số: 627/QĐ-BTC	*Hà Nội, ngày 05 tháng 04 năm 2017*

QUYẾT ĐỊNH

Về việc sửa đổi, bổ sung một số điều của 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 3317/QĐ-BTC ngày 24/12/2014

BỘ TRƯỞNG BỘ TÀI CHÍNH

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 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 85/2016/NĐ-CP ngày 01/7/2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Nghị định số 215/2013/NĐ-CP ngày 23/12/2013 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Tài chính;

Căn cứ Thông tư số 161/2014/TT-BTC ngày 31/10/2014 của Bộ Tài chính quy định công tác bảo vệ bí mật nhà nước của ngành Tài chính;

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

QUYẾT ĐỊNH:

Điều 1. Sửa đổi, bổ sung một số điều của 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 3317/QĐ-BTC ngày 24/12/2014 như sau:

1. Bổ sung các khoản 15, 16, 17 vào sau Khoản 14 Điều 2 như sau:

"15. "Kết nối Internet": Kết nối mạng tới hệ thống mạng Internet nhằm cung cấp khả năng truy cập Internet hoặc cung cấp thông tin, dịch vụ ra Internet.

16. "Truy cập Internet": Việc tiếp cận, khai thác, sử dụng thông tin, tài liệu, ứng dụng, dịch vụ trên Internet.

17. Một số kỹ thuật đảm bảo an toàn mạng, an toàn kết nối, truy cập Internet:

- "Chống tấn công từ chối dịch vụ": Hệ thống ngăn chặn tác dụng của các cuộc tấn công trên mạng nhằm làm suy giảm hoặc gián đoạn hoạt động của một trang tin, ứng dụng, dịch vụ hoặc hệ thống mạng, dẫn đến người dùng không thể sử dụng trang tin, ứng dụng, dịch vụ hoặc hệ thống mạng này.

- "IDS/IPS": Viết tắt của cụm từ Intrusion Detection System/Intrusion Prevention System, là hệ thống phát hiện, ngăn chặn các hoạt động vào, ra trên hệ thống thông tin được bảo vệ có dấu hiệu gây hại hoặc vi phạm chính sách an toàn mạng."

- "Phát hiện, ngăn chặn tấn công có chủ đích": Phát hiện, ngăn chặn loại hình tấn công được thiết kế nhằm đột nhập vào một hệ thống thông tin cụ thể.

- "Proxy": Hệ thống làm nhiệm vụ chuyển tiếp yêu cầu truy cập Internet từ bên trong mạng nội bộ ra Internet, nhằm che giấu thông tin về thiết bị, máy tính đưa ra yêu cầu truy cập Internet.

- "Remote Desktop": Giải pháp đảm bảo an toàn truy cập Internet của người dùng thông qua việc thiết lập kết nối Internet từ máy chủ cài đặt phần mềm Remote Desktop Services thay cho từ máy tính làm việc của người dùng.

- "Tường lửa": Hệ thống cho phép hoặc không cho phép thiết lập kết nối mạng giữa thiết bị thuộc vùng mạng này và thiết bị thuộc vùng mạng khác theo chính sách an toàn mạng của đơn vị.

- "Tường lửa ứng dụng web": Hệ thống ngăn chặn các tấn công nhằm vào các điểm yếu của lớp ứng dụng web.

- "VDI": Viết tắt của cụm từ Virtual Desktop Infrastructure, là giải pháp cung cấp môi trường làm việc trên hệ thống ảo hóa, được vận dụng để đảm bảo an toàn truy cập Internet của người dùng thông qua việc thiết lập kết nối Internet từ hệ thống ảo hóa thay cho từ máy tính làm việc của người dùng.

2. Sửa đổi Điều 8 như sau:

"**Điều 8. Đảm bảo an toàn kết nối, truy cập Internet**

1. Cán bộ, công chức, viên chức các đơn vị thuộc Bộ Tài chính được truy cập Internet tại cơ quan cho các mục đích: Cập nhật thông tin tình hình kinh tế, chính trị, xã hội của Việt Nam và thế giới; Tra cứu văn bản quy phạm pháp luật và các tài liệu, thông tin tham khảo phục vụ công việc; Sử dụng các dịch vụ hành chính công; Giao dịch với các cơ quan, tổ chức liên quan tới công việc được giao; Nghiên cứu, học tập nâng cao trình độ.

2. Việc truy cập Internet của cán bộ, công chức, viên chức được thực hiện thông qua một hoặc một số cách thức sau: Thiết lập mạng riêng gồm các máy tính chỉ phục vụ truy cập Internet; Thiếp lập mạng không dây chỉ phục vụ truy cập Internet; Truy cập Internet từ máy tính làm việc.

3. Bảo đảm tính hiệu quả của việc truy cập Internet:

a) Áp dụng biện pháp quản lý truy cập Internet trong giờ làm việc (về thời gian và nội dung truy cập) nhằm tránh tình trạng truy cập Internet quá mức gây ảnh hưởng đến hiệu suất làm việc của cán bộ và lãng phí nguồn lực của cơ quan.

b) Giám sát lưu lượng và tối ưu hóa việc sử dụng đường truyền Internet của đơn vị.

4. Không kết nối Internet cho các trường hợp sau:

a) Máy tính sử dụng để đọc, soạn thảo, lưu trữ, in ấn văn bản thuộc bí mật nhà nước;

b) Máy tính xử lý thông tin trên hệ thống thông tin cấp độ 4 trở lên;

c) Máy tính phục vụ quản trị hệ thống thông tin;

d) Toàn bộ máy chủ và thiết bị công nghệ thông tin không phải máy tính ngoại trừ các hệ thống bắt buộc phải có giao tiếp với Internet (các hệ thống phục vụ truy cập Internet; cung cấp giao diện ra Internet của trang tin điện tử, dịch vụ công, thư điện tử; phục vụ cập nhật bản vá hệ điều hành, mẫu mã độc, mẫu điểm yếu, mẫu tấn công).

5. Áp dụng các biện pháp kỹ thuật đảm bảo an toàn kết nối, truy cập Internet:

a) Các biện pháp kỹ thuật tối thiểu: Trang bị tường lửa; Cài đặt phần mềm phòng, diệt mã độc và cập nhật bản vá hệ điều hành trên máy tính kết nối Internet.

b) Đối với truy cập Internet từ máy tính làm việc của cán bộ tại cơ quan Bộ, đơn vị cấp Trung ương thuộc Kho bạc Nhà nước và các Tổng cục thuộc Bộ, áp dụng một hoặc một số biện pháp nâng cao sau theo năng lực đầu tư, vận hành hệ thống kỹ thuật của đơn vị: Trang bị proxy, hệ thống lọc trang web theo phân loại và ngăn chặn truy cập các trang web nhiễm mã độc; Trang bị hệ thống phát hiện, ngăn chặn tấn công có chủ đích; Cách ly máy tính làm việc và mạng Internet bằng công nghệ VDI hoặc Remote Desktop.

c) Đối với truy cập Internet từ máy tính làm việc của cán bộ tại cơ quan cấp tỉnh, áp dụng một hoặc một số biện pháp nâng cao sau theo năng lực đầu tư, vận hành hệ thống kỹ thuật của đơn vị: Trang bị proxy; Trang bị hệ thống lọc trang web theo phân loại và ngăn chặn truy cập các trang web nhiễm mã độc; Cách ly máy tính làm việc và mạng Internet bằng công nghệ ảo hóa VDI hoặc Remote Desktop.

d) Đối với các trang tin điện tử, dịch vụ hành chính công và các ứng dụng phục vụ truy cập từ Internet, áp dụng các biện pháp bảo vệ sau: IDS/IPS; Tường lửa ứng dụng web; Đánh giá và khắc phục điểm yếu của hệ thống thông tin; Chống tấn công từ chối dịch vụ.

đ) Mạng riêng hoặc mạng không dây chỉ phục vụ truy cập Internet phải được cách ly với mạng làm việc (từ vùng mạng riêng hoặc mạng không dây này không truy cập được vào vùng mạng làm việc).

e) Các hệ thống kỹ thuật đảm bảo an toàn kết nối, truy cập Internet phải được bảo hành phần cứng, cập nhật mẫu mã độc, cập nhật mẫu tấn công liên tục. Công tác giám sát, vận hành các hệ thống này phải được thực hiện thường xuyên.

6. Cán bộ, công chức, viên chức các đơn vị thuộc Bộ Tài chính khi truy cập Internet có trách nhiệm:

a) Khai thác, sử dụng Internet tại cơ quan một cách hiệu quả.

b) Chủ động trang bị kiến thức về các rủi ro mất an toàn thông tin khi truy cập Internet.

c) Tuân thủ quy định, hướng dẫn của cơ quan về việc sử dụng Internet.

d) Không sử dụng các phương tiện truy cập Internet của cá nhân trên máy tính làm việc tại cơ quan (thiết bị wifi, 3G/4G)."

Điều 2. Quyết định này có hiệu lực từ ngày ký. Cục trưởng Cục Tin học và Thống kê tài chính, Thủ trưởng các đơn vị thuộc Bộ, công chức, viên chức Bộ Tài chính, các tổ chức và cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

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

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Vũ Thị Mai