Mới BG 22/12

BỘ TÀI CHÍNH
TỔNG CỤC THUẾ

Số: 2329/QĐ-TCT

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

Hà nội, ngày 16 tháng 12 năm 2014

QUYẾT ĐỊNH

Về việc ban hành Quy định đảm bảo an ninh, an toàn thông tin cho Hệ thống thông tin ngành Thuế

TỔNG CỤC TRƯỞNG TỔNG CỤC THUẾ

Căn cứ Quyết định số 115/2009/QĐ-TTg ngày 28/09/2009 của Thủ tướng Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Tổng cục Thuế trực thuộc Bộ Tài chính;

Căn cứ quyết định số 114/QĐ-BTC ngày 15/01/2013 của Bộ trưởng Bộ Tài chính về chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Cục Công nghệ thông tin trực thuộc Tổng cục Thuế;

Căn cứ Quyết định số 692/QĐ-TCT ngày 22/04/2013 của Tổng cục trưởng Tổng cục Thuế về Tổ chức và hoạt động của Cục Công nghệ thông tin trực thuộc Tổng cục Thuế;

Căn cứ Quyết định số 2615/QĐ-BTC ngày 19/10/2012 của Bộ trưởng Bộ Tài chính về việc đảm bảo an toàn thông tin trên môi trường máy tính và mạng máy tính;

Xét đề nghị của Cục trưởng Cục Công nghệ thông tin - Tổng cục Thuế,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo quyết định này "Quy định đảm bảo an ninh, an toàn thông tin cho Hệ thống thông tin ngành Thuế".

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày ký. Các đơn vị, công chức, viên chức, lao động hợp đồng trong ngành Thuế (bao gồm: Cơ quan Tổng cục Thuế, Cục Thuế các tỉnh/thành phố và các Chi cục Thuế trực thuộc) chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như điều 2;
- LĐ Tổng cục Thuế (để báo cáo);
- Lưu: VT, CNTT (3b).

KT. TỔNG CỤC TRƯỞNG
PHÓ TỔNG CỤC TRƯỞNG

Trần văn Phu

BỘ TÀI CHÍNH
TỔNG CỤC THUẾ

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

Hà Nội, ngày 16 tháng 12 năm 2014

QUY ĐỊNH ĐẢM BẢO AN NINH, AN TOÀN THÔNG TIN CHO HỆ THỐNG THÔNG TIN NGÀNH THUẾ

(Ban hành kèm theo Quyết định số 2329/QĐ-TCT, ngày 16 tháng 12 năm 2014 của Tổng cục trưởng Tổng cục Thuế)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Mục đích, phạm vi và đối tượng áp dụng

1. Mục đích

- Bảo vệ toàn diện, ngăn chặn các mối đe dọa, giảm thiểu các rủi ro do môi trường bị gián đoạn, lỗi của con người hoặc máy, các cuộc tấn công có mục đích làm mất an toàn thông tin; Đảm bảo an ninh, an toàn thông tin cho ngành Thuế trên môi trường mạng.

- Bảo vệ chống lại hành vi vô tình hay cố ý thay đổi trái phép, phá hủy, làm chậm trễ, trộm cắp, truy cập (khi không được quyền truy cập) gây thiệt hại cho hệ thống, dữ liệu, ứng dụng và thiết bị công nghệ thông tin.

2. Phạm vi áp dụng

Quy định này bao gồm các điều kiện tối thiểu phải tuân thủ nhằm đảm bảo an ninh, an toàn thông tin trên môi trường máy tính, mạng máy tính và hệ thống thông tin ngành Thuế.

3. Đối tượng áp dụng

- Các đơn vị, công chức, viên chức, lao động hợp đồng trong ngành Thuế (bao gồm: Cơ quan Tổng cục Thuế, Cục Thuế các tỉnh/thành phố và các Chi cục Thuế trực thuộc): Áp dụng đầy đủ quy định này.

- Cơ quan, tổ chức, cá nhân bên ngoài có kết nối trao đổi thông tin với ngành Thuế; Tham gia xây dựng và phát triển, duy trì hệ thống thông tin ngành Thuế: Áp dụng các quy định trong hoạt động trao đổi thông tin với ngành Thuế.

Điều 2. Giải thích từ ngữ

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

1. "An ninh, an toàn thông tin": Sự bảo vệ thông tin và hệ thống thông tin tránh bị truy cập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính toàn vẹn, tính bảo mật và tính khả dụng của thông tin.

2. "Hệ thống thông tin": Tập hợp thiết bị phần cứng, phần mềm và cơ sở dữ liệu của các đơn vị thuộc ngành Thuế được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin.

3. "Hệ thống quan trọng": Hệ thống thông tin có vai trò, ý nghĩa quan trọng đối với sự phát triển và quản lý của ngành Thuế, nếu bị phá hoại sẽ gây ảnh hưởng lớn tới hoạt động của ngành và lợi ích công cộng.

4. Mạng nội bộ cơ quan Tổng cục Thuế: Hệ thống mạng máy tính tại trụ sở cơ quan Tổng cục Thuế, phần mở rộng của mạng này tới trụ sở của các đơn vị thuộc Tổng cục đặt ngoài trụ sở cơ quan Tổng cục Thuế và Đại diện Văn phòng Tổng cục Thuế tại thành phố Hồ Chí Minh.

5. "Mã độc": Phần mềm có khả năng 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.

6. "Lỗ hổng bảo mật": Điểm yếu kỹ thuật trong hệ thống thông tin có thể bị khai thác làm mất tính an ninh, an toàn của thông tin.

7. "Rủi ro an ninh, an toàn thông tin": Khả năng thông tin mất an ninh, an toàn (không sẵn sàng, bị xâm phạm tính toàn vẹn, bị tiếp cận bởi các đối tượng không có thẩm quyền truy cập).

8. "Sự cố an ninh, an toàn thông tin": Sự kiện thông tin mất an ninh, an toàn.

9. "Dịch vụ đám mây": Là mô hình sử dụng điện toán các công nghệ máy tính và phát triển dựa vào mạng Internet, cho phép người sử dụng truy cập các dịch vụ công nghệ từ một nhà cung cấp nào đó.

10. Người sử dụng: Là công chức, viên chức, lao động hợp đồng trong ngành Thuế hoặc các cơ quan, tổ chức, cá nhân ngoài ngành Thuế sử dụng máy tính hoặc các thiết bị có kết nối vào mạng nội bộ của cơ quan Thuế để xử lý công việc.

11. Đối tác: Là đơn vị ký kết hợp đồng thực hiện xây dựng, triển khai, bảo hành, bảo trì,...hệ thống thông tin với ngành Thuế.

12. Tài sản Công nghệ thông tin (CNTT): bao gồm: tài sản vật lý, tài sản thông tin và tài sản phần mềm, trong đó:

+ Tài sản vật lý: Là các thiết bị CNTT, phương tiện truyền thông và các thiết bị phục vụ cho hoạt động của hệ thống thông tin.

+ Tài sản thông tin: Là các dữ liệu, tài liệu liên quan đến hệ thống thông tin. Tài sản thông tin được thể hiện bằng văn bản giấy hoặc dữ liệu điện tử.

+ Tài sản phần mềm: Bao gồm các phần mềm ứng dụng, phần mềm hệ thống, cơ sở dữ liệu và công cụ phát triển.

13. Dữ liệu: Là thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự...

14. Cơ sở dữ liệu (CSDL): Là tập hợp các dữ liệu được sắp xếp, tổ chức để truy cập, khai thác, quản lý và cập nhật thông qua công cụ điện tử.

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 hệ thống thông tin.

2. Đơn vị, người sử dụng thực hiện các công đoạn liên quan đến thông tin nêu tại khoản 1 điều này có trách nhiệm đảm bảo an ninh, an toàn thông tin cho hệ thống thông tin của đơn vị mình theo quy định này.

3. Người sử dụng 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.

Điều 4. Những hành vi bị nghiêm cấm

1. Vi phạm các quy định về quản lý, vận hành và sử dụng hệ thống mạng của ngành Thuế gây rối loạn hoạt động của hệ thống và các hành vi: đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập không dây của cá nhân vào hệ thống mạng nội bộ; trên cùng một thiết bị thực hiện đồng thời kết nối vào mạng nội bộ và kết nối Internet bằng thiết bị truy cập Internet của cá nhân (modem quay số, USB 3G, điện thoại di động, máy tính bảng).

2. Can thiệp trái phép, gây nguy hại, xóa, thay đổi, sửa chữa, làm sai lệch thông tin.

3. Phát tán thư rác, mã độc, thiết lập hệ thống thông tin giả mạo, lừa đảo trong hệ thống mạng của ngành Thuế; Lợi dụng sơ hở, điểm yếu của hệ thống thông tin để tấn công, chiếm quyền điều khiển trái phép đối với hệ thống.

4. Làm mất tác dụng của các biện pháp an toàn thông tin do đơn vị thiết lập và các hành vi: Tự ý thay đổi, gỡ bỏ các biện pháp an toàn thông tin cài đặt trên thiết bị công nghệ thông tin phục vụ công việc; Tự ý thay thế, tráo đổi các thành phần của máy tính phục vụ công việc.

5. Vi phạm Quy chế bảo vệ bí mật nhà nước của ngành Thuế trong quá trình sử dụng thiết bị công nghệ thông tin, trong đó bao gồm hành vi tiết lộ mật khẩu tài khoản truy cập hệ thống thông tin ngành Thuế cho các đối tượng không được phép sử dụng hoặc đánh cắp mật khẩu của người khác.

Chương II

QUY ĐỊNH CỤ THỂ

Điều 5. Đảm bảo an ninh, an toàn thiết bị; Vật lý và môi trường

1. Đảm bảo an ninh, an toàn vật lý và môi trường

a) Phạm vi kiểm soát:

- Phạm vi kiểm soát truy cập vật lý là khu vực, phương tiện xử lý và lưu trữ thông tin như Trung tâm dữ liệu Tổng cục Thuế (các thiết bị máy chủ, thiết bị lưu trữ, thiết bị mạng, bảo mật...); Phòng máy chủ Cục Thuế/Chi cục Thuế (các thiết bị máy chủ, thiết bị lưu trữ, thiết bị mạng, bảo mật...); Tủ chứa thiết bị mạng tại các tòa nhà; Các phòng vận hành, kiểm soát (quản trị) hệ thống; Văn phòng làm việc của các đơn vị...

b) Thực hiện kiểm soát:

- Đối với các tài sản cần bảo mật ở mức thông thường: Sử dụng vành đai bảo mật (ví dụ như tường, thẻ ra vào hoặc bàn tiếp tân...) để bảo vệ những khu vực chứa thông tin hoặc những phương tiện xử lý thông tin.

- Đối với các tài sản cần bảo mật ở mức cao: Sử dụng các biện pháp kiểm soát ra, vào một cách phù hợp để đảm bảo chỉ những người được sự đồng ý của lãnh đạo đơn vị mới được phép vào.

- Đối với phòng máy chủ và trung tâm dữ liệu: Phải có nội quy hoặc hướng dẫn làm việc; Có mô hình thiết kế hệ thống theo quy định; Yêu cầu phải thiết kế và thực hiện các phương pháp phòng chống hỏa hoạn, lũ lụt, động đất, cháy nổ

và những tai họa tự nhiên hoặc do con người gây ra; Hệ thống khóa phải giao cho ít nhất 02 người: 01 quản trị, 01 lãnh đạo phụ trách CNTT.

- Đối với việc di chuyển phòng máy chủ tại Cục Thuế, Chi cục Thuế không được thuê đơn vị bên ngoài ngành Thuế thực hiện để đảm bảo an toàn dữ liệu.

2. Đảm bảo an ninh, an toàn các thiết bị tài sản CNTT

- Tài sản CNTT phải được bố trí, lắp đặt tại các địa điểm an toàn và được bảo vệ để giảm thiểu những rủi ro do các đe dọa, hiểm họa từ môi trường và các xâm nhập trái phép.

- Thiết bị CNTT phải được bảo đảm về nguồn điện và các hệ thống hỗ trợ khi nguồn điện chính bị gián đoạn. Phải có biện pháp chống quá tải hay sụt giảm điện áp, chống sét lan truyền; Hệ thống máy phát điện dự phòng và hệ thống lưu điện đảm bảo thiết bị hoạt động liên tục.

- Các thiết bị thuộc hệ thống quan trọng phải được bảo dưỡng định kỳ và duy trì chế độ bảo hành liên tục hoặc có cơ chế sửa chữa, thay thế đáp ứng yêu cầu về mức độ sẵn sàng của hệ thống trong suốt thời gian sử dụng.

- Dây cáp cung cấp nguồn điện và dây cáp sử dụng trong truyền tải dữ liệu hay những dịch vụ hỗ trợ thông tin phải được bảo vệ khỏi sự xâm phạm hoặc hư hại.

- Tất cả các thiết bị lưu trữ dữ liệu trước khi loại bỏ hoặc tái sử dụng cho mục đích khác, phải được kiểm tra để đảm bảo các dữ liệu quan trọng và phần mềm có bản quyền lưu trữ trên các thiết bị này được xóa bỏ hoặc ghi đè không có khả năng khôi phục.

- Việc sửa chữa, bảo hành thiết bị CNTT do đơn vị bên ngoài thực hiện phải có sự giám sát của cán bộ thuộc bộ phận tin học nhằm đảm bảo an toàn, an ninh dữ liệu, tài nguyên trên máy tính.

- Thiết bị thông tin của đơn vị khi mang đi bảo hành, bảo dưỡng, sửa chữa phải tháo ổ cứng khỏi thiết bị hoặc xóa các thông tin, dữ liệu lưu trữ trên thiết bị (trừ trường hợp mang thiết bị đi khôi phục dữ liệu). Các thiết bị lưu trữ không sử dụng tiếp cho công việc của đơn vị (thanh lý, cho, tặng) phải được xóa nội dung bằng phần mềm hoặc bằng thiết bị hủy dữ liệu chuyên dụng.

- Tài sản CNTT chỉ được đưa ra bên ngoài đơn vị khi có sự cho phép của cấp có thẩm quyền.

- Các trang thiết bị dùng cho hoạt động nghiệp vụ lắp đặt bên ngoài trụ sở của đơn vị phải có biện pháp giám sát, bảo vệ an toàn phòng chống truy cập bất hợp pháp.

Điều 6. Tổ chức bộ máy đảm bảo an ninh, an toàn thông tin cho hệ thống thông tin ngành Thuế

- Thủ trưởng đơn vị:

+ Trực tiếp chỉ đạo công tác đảm bảo an ninh, an toàn thông tin cho hệ thống thông tin toàn đơn vị.

+ Phân công bộ phận và cá nhân đảm nhiệm trách nhiệm quản lý an ninh, an toàn thông tin cho hệ thống thông tin của đơn vị.

+ Tổ chức đào tạo, hướng dẫn thực hiện an ninh, an toàn thông tin trong đơn vị.

- Cá nhân trong đơn vị:

+ Tuân thủ các quy định về an ninh, an toàn thông tin.

+ Tham gia đầy đủ các buổi đào tạo, hướng dẫn thực hiện an ninh, an toàn thông tin do cơ quan, đơn vị tổ chức.

- Đối với tài sản CNTT của đơn vị:

+ Phân loại, sắp xếp thứ tự ưu tiên theo giá trị, độ nhạy cảm, mức độ quan trọng của tài sản, thời gian lưu trữ để có biện pháp bảo vệ phù hợp.

+ Gắn quyền sử dụng tài sản cho các cá nhân hoặc đơn vị cụ thể. Cá nhân, đơn vị sử dụng tài sản cần tuân thủ các quy định về quản lý, sử dụng tài sản hiện hành của ngành, đảm bảo tài sản được sử dụng đúng mục đích.

+ Thống kê, kiểm kê các loại tài sản CNTT tại đơn vị tối thiểu 01 lần/năm. Nội dung thống kê tài sản phải bao gồm các thông tin: Tên tài sản, Loại tài sản, Chủ tài sản, Giá trị, Mức độ quan trọng, Vị trí lắp đặt,...

Điều 7. Quản lý nhân sự đảm bảo an ninh, an toàn thông tin cho hệ thống thông tin ngành Thuế

1. Quản lý nhân sự nội bộ

a) Trong quá trình tuyển dụng: Việc tuyển dụng công chức, viên chức, lao động hợp đồng vào công tác trong ngành Thuế phải được thực hiện đúng theo quy định của Luật công chức, Luật viên chức, các văn bản quy phạm pháp luật hướng dẫn Luật và các quy định của Bộ Tài chính.

b) Trong quá trình làm việc: Đơn vị có trách nhiệm:

- Phổ biến, đào tạo và thường xuyên cập nhật các quy định, chính sách về đảm bảo an ninh, an toàn thông tin cho hệ thống thông tin tới công chức, viên chức, lao động hợp đồng. Tuyệt đối không soạn thảo, in ấn tài liệu mật từ máy tính có nối mạng (các đơn vị bố trí máy tính độc lập không kết nối với mạng bằng mọi hình thức để soạn thảo, in ấn các tài liệu mật theo quy định); Không

sao chép, lưu trữ tài liệu có tính chất mật dưới dạng số; Không chuyển tải tài liệu mật trên môi trường mạng.

- Hướng dẫn cán bộ đảm bảo an toàn trong việc sử dụng Internet, email, trao đổi dữ liệu với bên ngoài. Chỉ sử dụng hệ thống thư điện tử của ngành để trao đổi thông tin, tài liệu làm việc. Không sử dụng hệ thống thư điện tử khác, các phương tiện trao đổi thông tin công cộng trên Internet cho mục đích này. Không lưu trữ các dữ liệu quan trọng, tài liệu bí mật của cơ quan Nhà nước trên các loại thiết bị di động thông minh (điện thoại thông minh smart phone, máy tính bảng, thiết bị thu phát media,...).

- Thực hiện kiểm tra việc thi hành các quy định, chính sách về đảm bảo an ninh, an toàn thông tin cho hệ thống thông tin của công chức, viên chức, lao động hợp đồng thuộc đơn vị tối thiểu 01 lần/năm.

- Áp dụng các biện pháp kỷ luật đối với công chức, viên chức, lao động hợp đồng vi phạm quy định về đảm bảo an ninh, an toàn thông tin cho hệ thống thông tin.

- Những nội dung công việc quan trọng như cài đặt, cấu hình hệ thống an ninh mạng (thiết bị tường lửa, thiết bị phát hiện và ngăn chặn xâm nhập), thay đổi tham số hệ điều hành phải được thực hiện bởi ít nhất 02 người hoặc phải có người giám sát của đơn vị.

c) Nghỉ việc hoặc thuyên chuyển công tác:

- Xác định rõ trách nhiệm của công chức, viên chức, lao động hợp đồng và các bên liên quan về hệ thống thông tin.

- Lập biên bản bàn giao tài sản CNTT với công chức, viên chức, lao động hợp đồng.

- Thu hồi hoặc thay đổi quyền truy cập hệ thống thông tin của công chức, viên chức, lao động hợp đồng cho phù hợp với công việc được thay đổi.

2. Quản lý nhân sự bên ngoài

a) Trước khi hợp tác:

- Yêu cầu đối tác cung cấp danh sách nhân sự tham gia (nếu cần).

- Kiểm tra thông tin, tư cách pháp nhân, năng lực chuyên môn của nhân sự tham gia.

- Ký cam kết đảm bảo an ninh, an toàn thông tin với đối tác (nếu cần) theo mẫu *01-BM/QĐANTT/ANTT/TCT* (áp dụng đối với cá nhân) hoặc mẫu *02-BM/QĐANTT/ANTT/TCT* (áp dụng đối với tổ chức) Phụ lục I của Quy định này.

b) Trong quá trình hợp tác:

- Yêu cầu đối tác tuân thủ các quy định, chính sách về đảm bảo an ninh, an toàn thông tin của đơn vị.

- Giám sát việc thực hiện các quy định về đảm bảo an ninh, an toàn thông tin cho hệ thống thông tin đối với đối tác.

- Có biện pháp bảo vệ, mã hóa đối với các dữ liệu thông tin (cần bảo mật) khi trao đổi.

- Kiểm soát việc cung cấp dữ liệu, trao đổi thông tin với các đơn vị ngoài ngành. Việc cung cấp trao đổi thông tin phải được sự đồng ý của lãnh đạo đơn vị. Trường hợp cung cấp dữ liệu thông tin mật cho các đơn vị ngoài ngành phải yêu cầu đơn vị tiếp nhận thông tin ký cam kết bảo mật theo quy định.

- Các tài liệu quan trọng, tài liệu mật phải được đặt mật khẩu có độ phức tạp cao hoặc được lưu trữ trong một thư mục riêng được mã hóa bằng mật khẩu phức tạp.

- Trường hợp phát hiện vi phạm quy định đảm bảo an ninh, an toàn thông tin cho hệ thống thông tin của nhân sự bên ngoài, đơn vị cần:

+ Tạm dừng hoặc đình chỉ hoạt động của đối tác tùy theo mức độ vi phạm.

+ Thông báo chính thức các vi phạm về đảm bảo an ninh, an toàn thông tin của nhân sự cho đối tác.

+ Kiểm tra, xác định, lập báo cáo mức độ vi phạm và thông báo cho đối tác các thiệt hại xảy ra.

+ Thu hồi quyền truy cập của đối tác.

+ Trường hợp vi phạm nghiêm trọng, gây ảnh hưởng lớn tới hệ thống thông tin, làm thất thoát, ảnh hưởng tới uy tín và hình ảnh của đơn vị sẽ chuyển các cơ quan chức năng xử lý theo quy định của pháp luật.

c) Kết thúc quá trình hợp tác:

- Yêu cầu đối tác bàn giao lại tài sản thông tin sử dụng trong quá trình làm việc.

- Thực hiện cắt quyền truy cập hệ thống.

- Thay đổi hoặc khóa mật khẩu truy cập của đối tác.

Điều 8. Quản lý vận hành và truyền thông

1. Quản lý vận hành

- Ban hành và triển khai quy trình quản lý vận hành các hệ thống thông tin nhằm đảm bảo vận hành chính xác và an toàn các trang thiết bị xử lý thông tin.

- Các phần mềm ứng dụng, phần mềm hệ thống phải đảm bảo yêu cầu về an ninh, an toàn thông tin được quy định tại Quy định này trước khi đưa vào vận hành chính thức.

- Kiểm soát sự thay đổi của hệ thống thông tin gồm: Phiên bản phần mềm, cấu hình phần cứng, cấu hình hệ thống, tài liệu, quy trình vận hành; Có phương án dự phòng cho việc phục hồi nếu sự thay đổi không thành công hoặc gặp các sự cố không dự tính được; Ghi chép lại các thay đổi; Lập kế hoạch thực hiện và kiểm tra, thử nghiệm sự thay đổi trước khi áp dụng chính thức.

- Hệ thống thông tin đưa vào vận hành cần đáp ứng các yêu cầu sau:

+ Tách biệt với môi trường phát triển và môi trường kiểm tra, thử nghiệm.

+ Chỉ được phép kết nối Internet khi áp dụng một số giải pháp an ninh thông tin như thiết bị tường lửa, máy chủ proxy truy cập Internet, máy trạm được cài đặt phần mềm diệt virus của ngành.

+ Không cài đặt các công cụ, phương tiện phát triển trên hệ thống vận hành chính thức.

+ Trung tâm dữ liệu, phòng giám sát hệ thống, máy chủ của các Cục Thuế đảm bảo vận hành theo yêu cầu của Quy định này và các quy định hiện hành của ngành.

- Đối với hệ thống tác nghiệp: Các tác vụ cập nhật, chỉnh sửa dữ liệu, truy cập hệ thống phải được lưu vết, sẵn sàng cho kiểm tra, kiểm soát khi cần thiết.

2. Quản lý các dịch vụ do đối tác cung cấp

- Có kế hoạch giám sát và kiểm tra các dịch vụ do đối tác cung cấp, đảm bảo khả năng hoạt động tốt, đáp ứng theo thỏa thuận/hợp đồng đã ký kết.

- Đảm bảo triển khai, duy trì các biện pháp an ninh, an toàn thông tin của dịch vụ do đối tác cung cấp.

- Quản lý các thay đổi đối với các dịch vụ do đối tác cung cấp bao gồm: Nâng cấp phiên bản mới; Thay thế giải pháp kỹ thuật; Các công cụ và môi trường phát triển mới. Thực hiện đánh giá đầy đủ các tác động của việc thay đổi, đảm bảo an toàn và kiểm soát được rủi ro trước khi đưa vào sử dụng.

3. Quản lý lập kế hoạch và chấp nhận hệ thống

- Xây dựng các yêu cầu, tiêu chuẩn như hiệu năng, thời gian khắc phục sự cố, đảm bảo tính liên tục, đào tạo và chuyển giao kỹ thuật đối với nội dung thay đổi, thực hiện kiểm tra, đánh giá khả năng đáp ứng của hệ thống thông tin mới xây dựng hoặc nâng cấp trước khi đưa vào áp dụng chính thức.

- Giám sát và tối ưu hiệu suất của hệ thống thông tin; Lập kế hoạch về hiệu suất, dung lượng của hệ thống thông tin trong tương lai nhằm đảm bảo tiêu chuẩn cần thiết.

4. Quản lý sao lưu, phục hồi dữ liệu

- Đơn vị phải có thiết bị và quy trình, nhân sự phục vụ công tác sao lưu dữ liệu phòng ngừa sự cố cho các hệ thống thông tin quan trọng.

- Lập danh sách các dữ liệu cần được sao lưu, có phân loại theo thời gian lưu trữ, thời gian sao lưu, phương pháp sao lưu và thời gian kiểm tra phục hồi hệ thống từ dữ liệu sao lưu.

- Dữ liệu sao lưu phải được lưu trữ an toàn, phải được kiểm soát và đối chiếu sau khi sao lưu. Thường xuyên kiểm tra kết quả thực hiện việc sao lưu dữ liệu của hệ thống đảm bảo việc sao lưu thành công và đảm bảo sẵn sàng cho việc sử dụng khi cần. Kiểm tra, phục hồi hệ thống từ dữ liệu sao lưu tối thiểu 06 tháng/lần.

- Định kỳ sao lưu toàn bộ dữ liệu. Quản trị hệ thống thực hiện sao lưu ra máy trạm riêng hoặc thiết bị lưu trữ bên ngoài đối với các dữ liệu quan trọng, có mức độ ảnh hưởng lớn tới hoạt động của hệ thống thông tin của đơn vị và cần thực hiện tối thiểu 01 tuần/lần. Có biện pháp bảo vệ dữ liệu được sao lưu trên máy trạm và thiết bị lưu trữ bên ngoài tránh thất thoát dữ liệu.

5. Quản lý an ninh mạng

a) Thực hiện việc quản lý và kiểm soát mạng nhằm ngăn ngừa các hiểm họa và duy trì an toàn cho các hệ thống, ứng dụng sử dụng mạng:

- Có sơ đồ logic và vật lý về thiết kế hệ thống mạng theo quy định.

- Hệ thống mạng nội bộ tại các Cục Thuế và các Chi cục Thuế có từ 200 người sử dụng trở lên phải được bảo vệ bằng tường lửa. Các Chi cục Thuế không có thiết bị tường lửa phải kết nối Internet thông qua hệ thống quản lý kết nối Internet (Firewall, Proxy, Web Gateway) tại Cục Thuế.

- Phân chia hệ thống mạng nội bộ tại Cục Thuế thành các vùng mạng theo phạm vi truy cập và kiểm soát truy cập giữa các vùng bằng tường lửa. Mạng nội bộ 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 sử dụng hoặc máy chủ).

+ Vùng mạng máy chủ nội bộ.

+ Vùng mạng người sử dụng, 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).

- Vô hiệu hoá tất cả các dịch vụ không sử dụng tại từng vùng mạng.

- Che giấu và tránh truy cập trực tiếp các địa chỉ mạng bên trong từ bên ngoài (Internet, hạ tầng truyền thông ngành Thuế).

- Cài đặt các bản cập nhật, vá lỗi đúng hạn cho 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 hoạt động liên tục của tường lửa.

- Rà soát việc cài đặt phần mềm diệt virus cho toàn bộ máy chủ, máy trạm tại Cục Thuế và các Chi cục Thuế. Theo dõi hàng ngày tình trạng hoạt động của phần mềm trên máy chủ, máy trạm nhằm đảm bảo phần mềm luôn được kết nối đến máy chủ quản trị diệt virus và được cập nhật mẫu virus mới nhất.

- Thực hiện thay đổi ngay mật khẩu đối với các tài khoản quản trị hệ thống, ứng dụng đảm bảo mật khẩu có độ phức tạp cao, định kỳ thực hiện thay đổi mật khẩu theo quy định.

- Tăng cường theo dõi tình hình virus tại Cục Thuế và Chi cục Thuế, xử lý triệt để các nguồn lây nhiễm virus. Đối với các trường hợp không xử lý được, thực hiện cách ly khỏi mạng nội bộ và báo cáo Tổng cục để có phương án xử lý. Không kết nối vào mạng nội bộ các máy tính chưa được cài phần mềm diệt virus.

- Thực hiện việc cập nhật các bản vá lỗ hổng bảo mật có mức độ nguy hiểm cao (critical) cho các máy trạm qua máy chủ Microsoft WSUS.

- Đặt tên máy trạm theo đúng quy định, join domain, sử dụng tài khoản domain khi làm việc, tuyệt đối không sử dụng tài khoản quản trị (Administrator) hoặc thuộc nhóm quản trị (nhóm Administrators) để tránh bị chiếm quyền điều khiển, lây nhiễm và phát tán virus trong mạng nội bộ.

- Rà soát việc cài đặt các phần mềm trên máy tính người sử dụng đúng theo quy định, dỡ bỏ các phần mềm lạ, phần mềm bẻ khóa, phần mềm không bản quyền.

- Hệ thống mạng không dây được thiết lập và quản lý phải đáp ứng các điều kiện tối thiểu sau:

+ Thiết bị phần cứng phải có chứng nhận Wi-Fi theo tiêu chuẩn hiện hành.

+ Áp dụng mã hoá dữ liệu truyền nhận sử dụng thuật toán mã hoá an toàn.

+ Người sử dụng mạng không dây phải được cung cấp định danh duy nhất và xác thực qua kênh mã hoá.

+ Các điểm truy cập không dây (thiết bị phát sóng làm cầu nối giữa mạng có dây và không dây) của đơn vị phải được bảo vệ tránh bị tiếp cận trái phép.

b) Sử dụng các công cụ để dò tìm và phát hiện kịp thời các điểm yếu, lỗ hổng và các truy cập bất hợp pháp vào hệ thống mạng. Thường xuyên kiểm tra, phát hiện những kết nối, trang thiết bị, phần mềm cài đặt bất hợp pháp vào hệ thống mạng.

c) Thực hiện các biện pháp nhằm tăng cường bảo vệ hệ thống mạng, bảo mật hệ thống dữ liệu của cơ quan, kiểm soát việc ra vào, tiếp cận các vùng chứa thông tin, dữ liệu của đơn vị (phòng máy chủ, hệ thống mạng, phòng lưu trữ hồ sơ). Sử dụng biện pháp kiểm soát việc kết nối các thiết bị ngoại vi (máy tính để bàn, máy tính xách tay, điện thoại di động, thiết bị phát sóng không dây...) vào mạng nội bộ.

d) Không được phép truy cập từ xa hệ thống mạng nội bộ trừ mục đích quản trị hệ thống. Xác định và ghi rõ các tính năng an toàn, mức độ bảo mật và yêu cầu quản lý trong các thỏa thuận đối với dịch vụ mạng do đối tác cung cấp.

6. Quản lý các thiết bị lưu trữ

- Các thiết bị lưu trữ (ổ cứng máy chủ và máy trạm, USB, băng đĩa từ...) chứa dữ liệu đầu vào, đầu ra, tài liệu hệ thống cần được kiểm soát và bảo vệ về mặt vật lý.

- Phổ biến tới người sử dụng tại đơn vị về việc hạn chế sử dụng các thiết bị lưu trữ di động như USB, ổ cứng cắm ngoài, thẻ nhớ,...để tránh lây nhiễm virus từ bên ngoài. Thực hiện quét virus trước khi truy xuất dữ liệu trên thiết bị lưu trữ di động.

- Tất cả các thiết bị lưu trữ khi hết khấu hao, trước khi thanh lý phải được huỷ dữ liệu.

- Các thiết bị lưu trữ sau khi được hủy dữ liệu phải được dán nhãn để phân biệt với các thiết bị lưu trữ khác.

7. Quản lý trao đổi thông tin

- Đối với các đơn vị, cá nhân trong ngành Thuế thực hiện theo quy định hiện hành của Bộ Tài chính.

- Đối với các cơ quan, tổ chức, cá nhân ngoài ngành Thuế thực hiện theo quy định tại khoản 2 Điều 7 Quy định này.

8. Quản lý dịch vụ công và giao dịch trực tuyến

- Có biện pháp bảo vệ thông tin trong giao dịch trực tuyến nhằm chống lại các hoạt động gian lận, sửa đổi trái phép:

+ Giao thức truyền thông phải được mã hóa.

+ Sử dụng các phương thức xác thực mạnh như xác thực đa thành phần hoặc chữ ký số cho các thành viên tham gia giao dịch, truy cập hệ thống.

- Thông tin trong các giao dịch trực tuyến phải được truyền đầy đủ, đúng địa chỉ, tránh bị sửa đổi, tiết lộ hoặc nhân bản một cách trái phép.

- Thông tin công khai trên các hệ thống thông tin phải được bảo vệ, nhằm ngăn chặn sự sửa đổi trái phép.

- Không để dữ liệu mật/quan trọng trên các dịch vụ đám mây ngoài Internet, chỉ cho phép để trên dịch vụ đám mây do Tổng cục Thuế triển khai.

9. Quản lý giám sát và ghi nhật ký hoạt động CNTT

- Thực hiện giám sát và ghi nhật ký hoạt động CNTT theo quy định chung của ngành.

- Các chức năng ghi nhật ký và thông tin nhật ký, chống giả mạo và truy cập trái phép phải được bảo vệ.

- Nhật ký hệ thống ghi lại các hoạt động CNTT không được phép chỉnh sửa hay xóa dữ liệu với bất kỳ lý do nào.

Điều 9. Quản lý truy cập

1. Quản lý truy cập người sử dụng

- Xây dựng và thực hiện các quy định về quản lý truy cập đối với người sử dụng, nhóm người sử dụng, đảm bảo đáp ứng yêu cầu nghiệp vụ và yêu cầu an toàn, bảo mật. Quy định về quản lý truy cập bao gồm các nội dung cơ bản sau:

a) Đăng ký, cấp phát quyền truy cập của người sử dụng:

- Khi người sử dụng có nhu cầu tạo tài khoản cá nhân trên hệ thống phải lập phiếu yêu cầu và được phê duyệt bởi lãnh đạo đơn vị hoặc người có thẩm quyền.

- Cấp phát quyền truy cập, sử dụng và khai thác ứng dụng; Tài nguyên trên mạng phải đảm bảo chặt chẽ, đúng mục đích sử dụng. Mỗi người sử dụng hệ thống chỉ được cấp một tài khoản và được phân quyền đủ để thực hiện nhiệm vụ được phân công.

b) Kiểm soát truy cập và xác thực người sử dụng:

- Việc quản lý, xác thực được người sử dụng truy nhập trên hệ thống đảm bảo đầy đủ thông tin người sử dụng hệ thống bao gồm: Họ tên, chức vụ, đơn vị công tác, số điện thoại,... trên hệ thống CSDL.

- Người sử dụng chỉ đăng nhập vào ứng dụng và khai thác dữ liệu bằng tài khoản được cấp. Nghiêm cấm dò tìm mật khẩu, sử dụng tài khoản của người khác để vào ứng dụng và khai thác dữ liệu.

- Kiểm tra và loại bỏ kịp thời tài khoản của người sử dụng hệ thống đã chuyển công tác, nghỉ hưu, hết hạn sử dụng hoặc không còn làm việc tại đơn vị trên hệ thống và cập nhật trên các tài liệu liên quan.

- Tạm dừng quyền sử dụng đối với tài khoản của người sử dụng đã được đăng ký trên hệ thống nhưng không làm việc trong hệ thống từ 60 ngày trở lên.

- Giới hạn số lần đăng nhập không thành công vào hệ thống là 05 lần. Sau 05 lần không đăng nhập thành công, tài khoản sẽ bị khóa trong 30 phút.

- Phát hiện và xử lý kịp thời những trường hợp người sử dụng truy nhập bất hợp pháp hoặc thao tác vượt quá giới hạn được giao.

c) Quản lý, cấp phát mật khẩu:

- Quản lý mật khẩu thực hiện theo Quy chế quản lý, triển khai, vận hành hạ tầng hệ thống công nghệ thông tin của ngành.

- Triển khai chính sách mật khẩu phức tạp trên hệ thống AD cho người sử dụng tại Cục Thuế và Chi cục Thuế.

d) Rà soát quyền truy cập:

- Quyền truy cập của mỗi cá nhân cần được rà soát định kỳ (tối thiểu 03 tháng/lần) hoặc ngay sau khi có sự thay đổi, luân phiên, luân chuyển, bổ nhiệm, miễn nhiệm vị trí công tác của công chức, viên chức.

2. Trách nhiệm người sử dụng

- Người sử dụng khi được cấp quyền truy cập phải sử dụng mật khẩu đúng quy định, giữ bí mật mật khẩu, định kỳ thay đổi mật khẩu (tối thiểu 03 tháng/lần), thoát khỏi hệ thống khi không làm việc hoặc tạm thời không làm việc trên hệ thống.

- Không truy cập và sử dụng hộp thư của người khác; Không giả mạo thư điện tử của người khác. Chỉ được phép truy cập vào hộp thư của người khác để xem nội dung thông tin khi được ủy quyền, hoặc được phép của lãnh đạo đơn vị quản lý.

6. Kiểm soát thiết bị di động và làm việc từ xa

- Khi người sử dụng có nhu cầu truy cập từ xa, căn cứ vào vị trí làm việc, tính chất công việc sẽ được phân quyền truy cập theo từng cấp độ. Việc truy cập bắt buộc sử dụng các giải pháp bảo mật như phương pháp xác thực nhiều yếu tố.

- Trường hợp bộ phận hỗ trợ người sử dụng hoặc cán bộ quản trị tại cơ quan Thuế các cấp có yêu cầu truy cập từ xa vào máy tính của người sử dụng để phục vụ công tác hỗ trợ thì phải được sự đồng ý của người sử dụng.

- Rà soát và thực hiện cấu hình trên hệ thống không cho phép kết nối các thiết bị di động thông minh vào mạng nội bộ của đơn vị.

- Không sử dụng các thiết bị di dộng thông minh để lưu trữ các tài liệu có nội dung bí mật và không cắm trực tiếp các thiết bị này vào máy tính tại cơ quan.

- Không mang các thiết bị di động thông minh vào các cuộc họp có nội dung bí mật.

- Hạn chế tối đa việc sử dụng các thiết bị thông minh tại nơi làm việc.

- Tất cả kết nối từ xa của người sử dụng tới mạng ngành Thuế phải được ghi vết (log) tối thiểu 03 tháng để theo dõi.

Điều 10. Phát triển, duy trì hệ thống thông tin

1. Yêu cầu về an ninh, an toàn thông tin cho hệ thống thông tin

- Khi xây dựng hệ thống thông tin mới hoặc nâng cấp hệ thống thông tin hiện tại, phải đưa ra các yêu cầu về đảm bảo an ninh, an toàn thông tin đồng thời với việc đưa ra các yêu cầu kỹ thuật, nghiệp vụ.

2. Đảm bảo an ninh, an toàn thông tin các ứng dụng do đơn vị phát triển hoặc thuê phát triển

- Mã hoá thông tin bí mật hoặc nhạy cảm bằng thuật toán mã hoá an toàn. Cần lựa chọn các giải pháp mã hóa thông tin cho phù hợp với yêu cầu của cấu trúc ứng dụng và phù hợp với giải pháp mã hoá của ngành.

- Đảm bảo hoạt động ổn định của các thông tin liên kết từ các ứng dụng liên quan đến ứng dụng đang xây dựng.

- Với các dự án nâng cấp ứng dụng, mã nguồn dùng để nâng cấp ứng dụng phải do người quản lý ứng dụng cung cấp. Các mã nguồn thay đổi trong quá trình nâng cấp cần có chú thích các thông tin như ngày thay đổi, nội dung thay đổi, người thay đổi hoặc ghi chú (nếu có).

- Trước khi triển khai, ứng dụng phải được kiểm thử nhằm đảm bảo chức năng, hiệu năng, bảo mật.

- Kiểm tra tính hợp lệ của dữ liệu đầu vào và đầu ra để đảm bảo dữ liệu chính xác và phù hợp.

- Cung cấp tài khoản người sử dụng nhằm kiểm thử hoạt động của hệ thống ứng dụng. Sau khi kết thúc quá trình kiểm thử, đảm bảo các tài khoản người sử dụng và dữ liệu nhập thử phải được xóa sạch trên hệ thống.

- Trong quá trình triển khai, phải sử dụng tài khoản riêng cho việc triển khai để truy cập vào các máy chủ cài đặt hệ thống. Kết thúc quá trình triển khai, cần đảm bảo các tài khoản truy cập các máy chủ phục vụ triển khai phải được gỡ bỏ.

- Thực hiện kiểm soát việc cài đặt phần mềm trên các máy chủ, máy tính của người sử dụng, thiết bị mạng đang hoạt động thuộc hệ thống mạng nội bộ.

- Khi chưa được sự đồng ý bằng văn bản của Tổng cục Thuế, đối tác không được phép sử dụng hoặc cung cấp cho các đơn vị khác mã nguồn hoặc phần mềm do đối tác xây dựng nhưng thuộc bản quyền của Tổng cục Thuế.

- Đối tác xây dựng ứng dụng cho Tổng cục Thuế không được phép chỉnh sửa, bổ sung thêm các chức năng ngoài nội dung đã được thống nhất giữa hai bên, ngoại trừ trường hợp có sự đồng ý bằng văn bản của Tổng cục Thuế.

- 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. Mã nguồn và tài liệu liên quan tới chương trình được người quản lý lưu giữ trên hệ thống quản lý phiên bản. Người quản lý kiểm soát và bàn giao mã nguồn cho đối tác thực hiện khi có yêu cầu nâng cấp hoặc cung cấp ra bên ngoài.

- Đảm bảo ứng dụng là duy nhất và có bản quyền sở hữu của cơ quan Thuế.

3. Đảm bảo an ninh, an toàn thông tin cho ứng dụng, phần mềm mua 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, an toàn 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 11. Quản lý sự cố do mất an ninh, an toàn thông tin cho hệ thống thông tin

- 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.

- Đơn vị phải phân công nhân sự quản lý an toàn, an ninh thông tin trên môi trường máy tính và mạng máy tính (bao gồm công tác giám sát theo dõi hoạt động của hệ thống, kiểm tra việc thực hiện quy định này tại đơn vị).

- Quy định rõ trách nhiệm báo cáo của công chức, viên chức, lao động hợp đồng và đối tác về sự cố CNTT.

- Trường hợp khẩn cấp, đơn vị cần lập tức báo cáo tình hình sự cố đến người có thẩm quyền và các bên liên quan để có biện pháp khắc phục trong thời gian sớm nhất.

- Phát hiện kịp thời các hành vi, hiện tượng, sự cố bất thường trên hệ thống để báo cáo các cấp có thẩm quyền và có phương án xử lý phù hợp. Tố giác những hành vi làm mất an ninh, an toàn thông tin cho hệ thống thông tin.

- Quá trình xử lý sự cố phải được ghi chép và lưu trữ tại đơn vị.

- Thu thập, ghi chép, bảo toàn bằng chứng, chứng cứ phục vụ cho việc kiểm tra, xử lý, khắc phục và phòng ngừa sự cố. Đối với những trường hợp sự cố về CNTT có liên quan tới pháp luật, đơn vị có trách nhiệm thu thập và cung cấp chứng cứ cho cơ quan có thẩm quyền.

- Các hệ thống an ninh mạng (cập nhật bản vá hệ điều hành, phòng diệt mã độc, 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.

- Thực hiện quản lý sự cố an ninh, an toàn thông tin: Thiết lập quy trình báo cáo sự cố an ninh, an toàn thông tin cho các cấp quản lý thuộc đơn vị; Phân tích, xác định nguyên nhân của sự cố, biện pháp khắc phục và ngăn ngừa tái diễn; Tổng hợp thông tin về các sự cố trong báo cáo an ninh, an toàn thông tin định kỳ của đơn vị.

Điều 12. Đảm bảo tính liên tục đối với các hệ thống và ứng dụng quan trọng

1. Đảm bảo hoạt động liên tục

- Căn cứ quy mô và mức độ của từng hệ thống thông tin đối với hoạt động của đơn vị, xác định các hệ thống và ứng dụng quan trọng.

- Định kỳ tối thiểu 06 tháng/lần phải kiểm tra, thử nghiệm, đánh giá và cập nhật nội dung các quy trình phù hợp với các quy định hiện hành, đảm bảo hoạt động liên tục của các hệ thống mạng và ứng dụng quan trọng.

- Các quy trình đảm bảo nghiệp vụ hoạt động liên tục phải được kiểm tra, đánh giá và cập nhật thường xuyên để đảm bảo tính hiệu quả.

2. Công tác dự phòng rủi ro

- 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 hoạt động liên tục của hệ thống.

- Tối thiểu 06 tháng/lần phải chuyển hoạt động từ hệ thống chính sang hệ thống dự phòng để đảm bảo tính đồng nhất và sẵn sàng của hệ thống dự phòng.

- Tối thiểu 03 tháng/lần tiến hành kiểm tra, đánh giá hoạt động của hệ thống dự phòng.

Điều 13. Thực hiện kiểm tra và báo cáo

1. Kiểm tra nội bộ hệ thống thông tin

- Các đơn vị phải tổ chức kiểm tra việc tuân thủ Quy định này tối thiểu mỗi năm một lần.

- Kết quả kiểm tra và các kiến nghị, đề xuất phải được ghi nhận và trình lãnh đạo đơn vị phê duyệt.

2. Báo cáo

Hàng năm trước ngày 05/12, Cục Thuế tổng hợp, báo cáo Tổng cục Thuế (qua Cục CNTT) bằng văn bản toàn bộ tình hình quản lý, triển khai, vận hành, khai thác sử dụng hạ tầng hệ thống Công nghệ thông tin (trong đó bao gồm cả hạng mục an ninh, an toàn thông tin) theo quy định nêu trên.

Chương III
TỔ CHỨC THỰC HIỆN

Điều 14. Trách nhiệm của các đơn vị

1. Cục CNTT

- Tổ chức thực hiện, hướng dẫn và kiểm tra việc thực hiện Quy định này tại các đơn vị trong ngành, các đơn vị có kết nối trao đổi thông tin với cơ quan Thuế.

- Tổng hợp tình hình hoạt động của hệ thống thông tin ngành Thuế.

- Căn cứ vào tình hình triển khai và điều kiện thực tế, hàng năm Cục CNTT thực hiện rà soát, kiểm tra, đánh giá nội dung Quy định và chủ trì trình Tổng cục Thuế các sửa đổi, bổ sung Quy định (nếu có).

2. Các đơn vị thuộc, trực thuộc Tổng cục Thuế

- Tổ chức triển khai thực hiện Quy định tại đơn vị.

- Phối hợp với Cục CNTT trong việc triển khai, thực hiện Quy định.

- Phản ánh nhu cầu, vướng mắc trong quá trình triển khai, thực hiện Quy định tại đơn vị tới Cục CNTT để phối hợp xử lý kịp thời.

- Hướng dẫn, kiểm tra việc thực hiện Quy định tại đơn vị và các đơn vị ngoài ngành có kết nối trao đổi thông tin với mạng nội bộ đơn vị.

3. Các đơn vị ngoài ngành Tài chính khi tham gia trao đổi thông tin với cơ quan Thuế

- Cung cấp danh sách nhân sự tham gia.

- Tuân thủ các quy định về an ninh, an toàn thông tin của cơ quan Thuế.

- Có thỏa thuận an ninh, an toàn thông tin với cơ quan Thuế (nếu được yêu cầu) theo mẫu 02-BM/QĐANTT/ANTT/TCT Phụ lục I của Quy định này.

- Bàn giao lại tài sản thông tin cho cơ quan Thuế khi kết thúc công việc.

Điều 15. Trách nhiệm của cá nhân

- Công chức, viên chức, lao động hợp đồng trong ngành Thuế có trách nhiệm tuân thủ Quy định này.

- Trong quá trình triển khai, thực hiện nếu có vướng mắc, người sử dụng cần phản ánh kịp thời với Thủ trưởng đơn vị để gửi về Tổng cục Thuế (qua Cục CNTT) để xem xét, sửa đổi, bổ sung Quy định cho phù hợp.

Điều 16. Xử lý vi phạm

Các đơn vị, công chức, viên chức, lao động hợp đồng trong ngành Thuế vi phạm Quy định này thì tuỳ theo tính chất, mức độ vi phạm bị xử lý kỷ luật hoặc các hình thức xử lý khác theo quy định của ngành Thuế và Luật cán bộ, công chức.

Cơ quan, tổ chức, cá nhân bên ngoài có kết nối trao đổi thông tin với ngành Thuế vi phạm Quy định này thì tùy theo tính chất, mức độ vi phạm xem xét xử lý theo quy định của ngành Thuế hoặc quy định của pháp luật nếu xét thấy mức độ vi phạm là nghiêm trọng.

KT. TỔNG CỤC TRƯỞNG

PHÓ TỔNG CỤC TRƯỞNG

BỘ TÀI CHÍNH

TỔNG CỤC THUẾ

Trần Văn Phu

