BỘ TÀI CHÍNH
TỔNG CỤC THUẾ

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

Số: 1731 /QĐ-TCT

Hà Nội, ngày 08 tháng 11 năm 2024

QUYẾT ĐỊNH
Ban hành Quy chế An toàn thông tin mạng và An ninh mạng ngành Thuế

TỔNG CỤC TRƯỞNG TỔNG CỤC THUẾ

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

Căn cứ Luật Bảo vệ bí mật nhà nước ngày 15 tháng 11 năm 2018;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Nghị định số 142/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về ngăn chặn xung đột thông tin trên mạng;

Căn cứ Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ về việc quy định chi tiết một số điều của Luật An ninh mạng;

Căn cứ Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về bảo vệ dữ liệu cá nhân;

Căn cứ Quyết định số 41/2018/QĐ-TTg ngày 25/9/2018 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 15/2021/QĐ-TTg ngày 30/3/2021 của Thủ tướng Chính phủ sửa đổi, bổ sung Khoản 1 Điều 3 Quyết định số 41/2018/QĐ-TTg ngày 25/9/2018 của Thủ tướng Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Tổng cục Thuế thuộc Bộ Tài chính;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ ban hành Quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng Quốc gia;

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;

Căn cứ Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và

Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định số 1013/QĐ-BTC ngày 19/5/2023 của Bộ trưởng Bộ Tài chính Ban hành Quy chế An toàn thông tin mạng và An ninh mạng Bộ Tài chính;

Theo đề nghị của Cục trưởng Cục Công nghệ thông tin.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế An toàn thông tin mạng và An ninh mạng ngành Thuế.

Điều 2. Điều khoản thi hành và tổ chức thực hiện

1. Quyết định này có hiệu lực thi hành kể từ ngày ký và thay thế Quyết định số 2329/QĐ-TCT ngày 16/12/2014 của Tổng cục trưởng Tổng cục Thuế về quy định đảm bảo An toàn thông tin mạng và An ninh mạng ngành Thuế.

2. Trong trường hợp các văn bản quy phạm pháp luật dẫn chiếu tại văn bản này được sửa đổi, bổ sung hoặc thay thế thì thực hiện theo văn bản quy phạm pháp luật đã sửa đổi, bổ sung hoặc thay thế đó.

Điều 3. Cục trưởng Cục Công nghệ thông tin, Thủ trưởng các Cục/Vụ/đơn vị thuộc và trực thuộc Tổng cục Thuế, Cục trưởng Cục Thuế các tỉnh/thành phố trực thuộc Trung ương, các đơn vị có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- TCTr Mai Xuân Thành (để b/c);
- Cục THTK (để b/c);
- Website Tổng cục Thuế;
- Lưu: VT, CNTT.

(84;5)

KT. TỔNG CỤC TRƯỞNG
PHÓ TỔNG CỤC TRƯỞNG

BỘ TÀI CHÍNH TỔNG CỤC THUẾ

Đặng Ngọc Minh

BỘ TÀI CHÍNH
TỔNG CỤC THUẾ

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

QUY CHẾ
An toàn thông tin mạng và An ninh mạng ngành Thuế

(Kèm theo Quyết định số 1731 /QĐ-TCT ngày 08 tháng 11 năm 2024 của Tổng cục trưởng Tổng cục Thuế)

Chương I
QUY ĐỊNH CHUNG

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

1. Quy chế này quy định về công tác an toàn thông tin mạng và an ninh mạng của ngành Thuế.

2. Quy chế này áp dụng với:

a) Công chức, viên chức, người lao động thuộc ngành Thuế và các cơ quan, tổ chức, cá nhân bên ngoài tham gia xây dựng, phát triển, sử dụng, quản trị và vận hành hệ thống thông tin ngành Thuế hoặc có kết nối trao đổi thông tin với ngành Thuế.

b) Các hệ thống, ứng dụng, dịch vụ công nghệ thông tin do ngành Thuế cung cấp, các hệ thống thông tin được triển khai trên hạ tầng công nghệ thông tin ngành Thuế.

Điều 2. Giải thích từ ngữ sử dụng trong Quy chế

1. *An toàn an ninh mạng* là viết tắt của *An toàn thông tin mạng và an ninh mạng:* được sử dụng khi nội dung quy định tại Quy chế áp dụng đồng thời quy định của pháp luật về an toàn thông tin mạng và an ninh mạng.

2. *An toàn thông tin mạng* là sự bảo vệ thông tin, hệ thống thông tin trên mạng 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.

3. *An ninh mạng* là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh Quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

4. *Hệ thống mạng nội bộ* gồm hệ thống mạng có dây và hệ thống mạng không dây.

5. *Hệ thống mạng nội bộ Cục Thuế* gồm hệ thống mạng nội bộ triển khai tại cơ quan Cục Thuế và hệ thống mạng nội bộ triển khai tại các Chi cục Thuế.

6. *Hệ thống thông tin* là tập hợp phần cứng, phần mềm và cơ sở dữ liệu

được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên mạng.

7. *Thiết bị xử lý thông tin* là thiết bị dùng để tạo lập, xử lý, lưu trữ, truyền đưa thông tin dưới dạng điện tử (máy tính, máy in, điện thoại thông minh, thiết bị mạng, thiết bị an ninh mạng, camera giám sát và các thiết bị tương tự khác).

8. *Người dùng* là công chức, viên chức, người lao động tại các đơn vị thuộc ngành Thuế, cá nhân bên ngoài tham gia xây dựng, phát triển, sử dụng, quản trị và vận hành hệ thống thông tin ngành Thuế hoặc có sử dụng các dịch vụ do ngành Thuế cung cấp, có kết nối trao đổi thông tin với ngành Thuế.

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

1. Mục tiêu:

a) Bảo vệ thông tin, hệ thống thông tin của ngành Thuế 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.

b) Bảo đảm hoạt động trên không gian mạng của đơn vị, cá nhân thuộc ngành Thuế không gây phương hại đến an ninh Quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

2. Nguyên tắc bảo đảm an toàn an ninh mạng:

a) Tuân thủ quy định của pháp luật về an toàn an ninh mạng; bảo vệ bí mật nhà nước, bí mật công tác, dữ liệu cá nhân; giao dịch điện tử và các quy định khác có liên quan. Trường hợp có văn bản quy định cập nhật, thay thế hoặc quy định khác tại văn bản quy phạm pháp luật, quyết định của cấp có thẩm quyền cao hơn thì áp dụng quy định tại văn bản đó.

b) Các hoạt động về an toàn an ninh mạng hướng tới mục tiêu hỗ trợ triển khai hoạt động nghiệp vụ, giảm thiểu gây ảnh hưởng đến triển khai các hoạt động nghiệp vụ.

c) Phân cấp, ủy quyền trách nhiệm bảo đảm an toàn an ninh mạng phù hợp với tổ chức bộ máy và phương thức làm việc của ngành Thuế.

Chương II
PHÂN CÔNG NHIỆM VỤ BẢO ĐẢM AN TOÀN AN NINH MẠNG

Điều 4. Phân công thực hiện bảo đảm an toàn an ninh mạng theo quy định của pháp luật

1. Chủ quản hệ thống thông tin:

a) Tổng cục Thuế là chủ quản hệ thống thông tin theo quy định tại khoản 1 Điều 4 Quy chế An toàn thông tin mạng và An ninh mạng Bộ Tài chính ban hành kèm theo Quyết định số 1013/QĐ-BTC ngày 19/5/2023 của Bộ trưởng Bộ

Tài chính.

b) Trường hợp hệ thống thông tin triển khai theo yêu cầu của Ủy ban nhân dân thì chủ quản hệ thống thông tin do Ủy ban nhân dân quy định.

2. Đơn vị vận hành hệ thống thông tin:

a) Cục Công nghệ thông tin là đơn vị vận hành hệ thống thông tin do Tổng cục Thuế làm chủ quản (trừ hệ thống thông tin quy định tại điểm b, điểm c, điểm d khoản này).

b) Cục Thuế là đơn vị vận hành hệ thống thông tin:

- Hệ thống mạng nội bộ triển khai tại cơ quan Cục Thuế.
- Hệ thống thông tin do Cục Thuế tự triển khai.
- Hệ thống thông tin khác do Tổng cục Thuế phân cấp, uỷ quyền.

c) Chi cục Thuế là đơn vị vận hành hệ thống thông tin:

- Hệ thống mạng nội bộ triển khai tại Chi cục Thuế.
- Hệ thống thông tin do Chi cục Thuế tự triển khai.
- Hệ thống thông tin khác do Tổng cục Thuế phân cấp, uỷ quyền.

d) Đơn vị cung cấp dịch vụ thực hiện vai trò đơn vị vận hành hệ thống thông tin đang trong thời gian thuê dịch vụ công nghệ thông tin.

3. Đơn vị chuyên trách an toàn an ninh mạng:

a) Cục Công nghệ thông tin đảm nhận vai trò đơn vị chuyên trách an toàn an ninh mạng của Tổng cục Thuế.

b) Phòng An toàn thông tin thuộc Cục Công nghệ thông tin đảm nhận vai trò bộ phận chuyên trách an toàn an ninh mạng của Tổng cục Thuế.

4. Đơn vị chuyên trách về ứng cứu sự cố:

a) Cục Công nghệ thông tin đảm nhiệm vai trò đơn vị chuyên trách ứng cứu sự cố của Tổng cục Thuế.

b) Cục Công nghệ thông tin tham mưu, trình Tổng cục Thuế thành lập Đội ứng cứu sự cố.

5. Lực lượng bảo vệ an ninh mạng ngành Thuế bao gồm bộ phận chuyên trách an toàn an ninh mạng thuộc Cục Công nghệ thông tin và các đơn vị vận hành hệ thống thông tin.

6. Đơn vị, bộ phận được phân công đảm nhiệm vai trò bảo đảm an toàn an ninh mạng quy định từ khoản 1 đến khoản 5 Điều này thực hiện trách nhiệm theo quy định của pháp luật áp dụng cho vai trò tương ứng và theo quy định tại Quy chế này. Đối với hệ thống mạng nội bộ Cục Thuế, Cục Thuế là đầu mối vận hành thực hiện lập hồ sơ đề xuất cấp độ theo quy định tại khoản 2 Điều 10 của Quy chế này.

Điều 5. Phối hợp với những cơ quan/tổ chức có thẩm quyền

1. Tại Tổng cục Thuế: Cục Công nghệ thông tin là đầu mối phối hợp công tác với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn an ninh mạng; phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin; tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của cơ quan, tổ chức có thẩm quyền.

2. Tại Cục Thuế: Phòng Công nghệ thông tin là đầu mối phối hợp công tác với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn an ninh mạng; phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn an ninh mạng; tham gia các hoạt động bảo đảm an toàn an ninh mạng khi có yêu cầu của cơ quan, tổ chức có thẩm quyền.

Điều 6. Kiểm tra, đánh giá an toàn an ninh mạng

1. Kiểm tra, đánh giá việc tuân thủ quy định của pháp luật về an toàn an ninh mạng:

a) Cục Công nghệ thông tin trình Tổng cục tổ chức kiểm tra, đánh giá việc tuân thủ quy định của pháp luật về an toàn an ninh mạng của các đơn vị thuộc cơ quan Tổng cục Thuế, các Cục Thuế trong kế hoạch kiểm tra công tác ứng dụng công nghệ thông tin hàng năm hoặc kế hoạch kiểm tra theo chuyên đề, đột xuất về an toàn an ninh mạng.

b) Phòng Công nghệ thông tin trình Cục Thuế tổ chức kiểm tra, đánh giá việc tuân thủ quy định của pháp luật về an toàn an ninh mạng của các đơn vị thuộc và trực thuộc Cục Thuế trong kế hoạch kiểm tra công tác ứng dụng công nghệ thông tin hàng năm hoặc kế hoạch kiểm tra theo chuyên đề, đột xuất về an toàn an ninh mạng.

2. Kiểm tra, đánh giá phát hiện mã độc, lỗ hổng, điểm yếu và thử nghiệm xâm nhập hệ thống thông tin: thực hiện theo quy định tại khoản 2 Điều 9 Quy chế An toàn thông tin mạng và An ninh mạng Bộ Tài chính ban hành kèm theo Quyết định số 1013/QĐ-BTC ngày 19/5/2023 của Bộ trưởng Bộ Tài chính.

Điều 7. Phòng ngừa, phát hiện, ngăn chặn và xử lý hành vi xâm phạm an ninh mạng

1. Đơn vị chuyên trách an toàn an ninh mạng phối hợp với đơn vị vận hành hệ thống thông tin thực hiện các nhiệm vụ theo quy định của Luật An ninh mạng và Nghị định số 53/2022/NĐ-CP:

a) Triển khai biện pháp quản lý, kỹ thuật để phòng ngừa, phát hiện, ngăn chặn, gỡ bỏ thông tin trên các hệ thống thông tin do Tổng cục Thuế làm chủ quản có các nội dung: tuyên truyền chống phá Nhà nước; kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; làm nhục, vu khống.

b) Triển khai biện pháp quản lý, kỹ thuật để phòng ngừa, phát hiện, ngăn chặn hoạt động xâm nhập bất hợp pháp, hành vi gián điệp mạng, xâm phạm bí mật nhà nước, bí mật công tác, thông tin cá nhân và kịp thời báo cáo các cơ quan

chức năng để xử lý nếu cần thiết.

c) Triển khai biện pháp kỹ thuật để phòng ngừa, ngăn chặn hành vi tấn công mạng và hành vi có liên quan đến tấn công mạng đối với hệ thống thông tin. Thường xuyên rà soát, kiểm tra hệ thống thông tin nhằm loại trừ nguy cơ khủng bố mạng.

d) Phối hợp, hỗ trợ các đơn vị chức năng thuộc Bộ Công an về phòng, chống gián điệp mạng để thực hiện: bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, thông tin cá nhân trên hệ thống thông tin; xác định nguồn gốc tấn công mạng, thu thập chứng cứ khi xảy ra tấn công mạng, xâm phạm hoặc đe dọa xâm phạm chủ quyền, lợi ích, an ninh Quốc gia, gây tổn hại nghiêm trọng trật tự, an toàn xã hội; gỡ bỏ các nội dung buộc phải gỡ bỏ theo quy định của pháp luật trên hệ thống thông tin.

2. Đơn vị chuyên trách an toàn an ninh mạng khi tiếp nhận tin báo về tình huống nguy hiểm về an ninh mạng, phát hiện hành vi vi phạm pháp luật về an ninh mạng hoặc khủng bố mạng liên quan đến hệ thống thông tin thuộc phạm vi quản lý của chủ quản hệ thống thông tin cần thông báo kịp thời cho Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Bộ Công an.

Điều 8. Phổ biến, tuyên truyền, đào tạo, bồi dưỡng về an toàn an ninh mạng

1. Cục Công nghệ thông tin, Cục Thuế tổ chức phổ biến, tuyên truyền, đào tạo nhận thức về an toàn an ninh mạng cho người sử dụng thông qua các văn bản, thư điện tử, trang thông tin điện tử, phần mềm hoặc thông qua các buổi hội thảo, hội nghị hoặc qua các phương tiện thông tin truyền thông.

2. Cục Công nghệ thông tin định kỳ hàng năm trình Tổng cục tổ chức đào tạo về an toàn an ninh mạng cho công chức, viên chức chuyên trách về công nghệ thông tin, an toàn thông tin; cử cán bộ tham gia đào tạo, bồi dưỡng về an toàn an ninh mạng.

Điều 9. Báo cáo an toàn an ninh mạng

1. Cục Công nghệ thông tin lập báo cáo theo quy định tại khoản 3 Điều 13 và Điều 14 Thông tư số 12/2022/TT-BTTTT trình Tổng cục gửi Cục Tin học và Thống kê tài chính trước ngày 20 tháng 12 hàng năm.

2. Cục Công nghệ thông tin lập báo cáo định kỳ 6 tháng (trước ngày 20 tháng 6), 01 năm (trước ngày 15 tháng 12) gửi Cơ quan điều phối Quốc gia theo quy định tại điểm c khoản 1 Điều 6 Thông tư số 20/2017/TT-BTTTT và gửi Cục Tin học và Thống kê tài chính.

Chương III
CẤP ĐỘ AN TOÀN HỆ THỐNG THÔNG TIN

Điều 10. Xây dựng cấp độ an toàn hệ thống thông tin

1. Việc xác định cấp độ hệ thống thông tin thực hiện theo quy định tại Điều 7, Điều 8, Điều 9, Điều 10, Điều 11 của Nghị định số 85/2016/NĐ-CP.

2. Xây dựng hồ sơ đề xuất cấp độ:

a) Trường hợp lập dự án đầu tư ứng dụng công nghệ thông tin, chủ đầu tư xây dựng thuyết minh đề xuất cấp độ, lồng ghép vào nội dung của báo cáo nghiên cứu khả thi gửi đơn vị thẩm định, trình cơ quan có thẩm quyền phê duyệt theo quy định của pháp luật về đầu tư.

b) Trường hợp thuê dịch vụ công nghệ thông tin, đơn vị chủ trì thuê dịch vụ xây dựng thuyết minh đề xuất cấp độ, lồng ghép vào nội dung của kế hoạch, dự án thuê dịch vụ, gửi đơn vị thẩm định, trình cơ quan có thẩm quyền phê duyệt theo quy định của pháp luật về thuê dịch vụ công nghệ thông tin.

c) Trường hợp hệ thống đang trong giai đoạn triển khai hoặc đang vận hành, đơn vị vận hành đề xuất cấp độ:

- Đối với hệ thống thông tin được đề xuất là cấp độ 1, cấp độ 2 và cấp độ 3: đơn vị vận hành hệ thống thông tin gửi hồ sơ đề xuất cấp độ tới đơn vị chuyên trách an toàn an ninh mạng để thẩm định.

- Đối với hệ thống thông tin được đề xuất là cấp độ 4 hoặc cấp độ 5: đơn vị vận hành hệ thống thông tin gửi hồ sơ đề xuất cấp độ tới đơn vị chuyên trách an toàn an ninh mạng để xin ý kiến chuyên môn về sự phù hợp của đề xuất cấp độ và phương án bảo đảm an toàn hệ thống thông tin theo cấp độ.

d) Tài liệu thuyết minh đề xuất cấp độ theo quy định tại Điều 8 Thông tư số 12/2022/TT-BTTTT.

3. Thẩm định hồ sơ đề xuất cấp độ:

a) Đối với hệ thống thông tin được đề xuất là cấp độ 1 hoặc cấp độ 2 hoặc cấp độ 3:

- Đơn vị chuyên trách an toàn an ninh mạng thực hiện thẩm định hồ sơ đề xuất cấp độ.

- Trường hợp đơn vị chuyên trách an toàn an ninh mạng đồng thời là đơn vị vận hành hệ thống thông tin, việc tổ chức thẩm định hồ sơ đề xuất cấp độ được thực hiện theo một trong các phương án sau đây:

+ Đơn vị chuyên trách an toàn an ninh mạng trình chủ quản hệ thống thông tin giao một đơn vị trực thuộc có đủ năng lực chủ trì, tổ chức thẩm định.

+ Đơn vị chuyên trách an toàn an ninh mạng trình chủ quản hệ thống thông tin thành lập Hội đồng thẩm định độc lập thực hiện nhiệm vụ thẩm định hồ sơ đề xuất cấp độ.

b) Đối với hệ thống thông tin được đề xuất là cấp độ 4 hoặc cấp độ 5:

- Đơn vị chuyên trách an toàn an ninh mạng có ý kiến chuyên môn về hồ sơ đề xuất cấp độ.

- Trường hợp đơn vị chuyên trách về an toàn thông tin đồng thời là đơn vị vận hành hệ thống thông tin, việc tổ chức có ý kiến chuyên môn về hồ sơ đề xuất cấp độ được thực hiện theo một trong các phương án sau đây:

+ Đơn vị chuyên trách an toàn an ninh mạng trình chủ quản hệ thống thông tin giao một đơn vị trực thuộc có đủ năng lực chủ trì thực hiện.

+ Đơn vị chuyên trách an toàn an ninh mạng trình chủ quản hệ thống thông tin thành lập Hội đồng đánh giá độc lập thực hiện.

- Sau khi có ý kiến của hội đồng đánh giá, đơn vị vận hành trình chủ quản hệ thống thông tin văn bản gửi Bộ Thông tin và Truyền thông thẩm định hồ sơ đề xuất cấp độ theo quy định tại khoản 3 Điều 12 Nghị định số 85/2016/NĐ-CP.

c) Trường hợp hồ sơ đề xuất cấp độ được đơn vị thẩm định xác định đáp ứng tiêu chí đưa vào Danh mục hệ thống thông tin quan trọng về an ninh Quốc gia (theo quy định tại Điều 10 Luật An ninh mạng và Điều 3 Nghị định số 53/2022/NĐ-CP), đơn vị vận hành trình Chủ quản hệ thống thông tin thực hiện theo quy định tại điểm b khoản 2 Điều 5 Quy chế An toàn thông tin mạng và An ninh mạng Bộ Tài chính ban hành kèm theo Quyết định số 1013/QĐ-BTC ngày 19/5/2023 của Bộ trưởng Bộ Tài chính.

d) Nội dung thẩm định hồ sơ đề xuất cấp độ theo quy định tại Điều 16 Nghị định số 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ.

4. Phê duyệt hồ sơ đề xuất cấp độ:

a) Đối với hệ thống thông tin được đề xuất là cấp độ 1 hoặc cấp độ 2: đơn vị chuyên trách an toàn an ninh mạng phê duyệt hồ sơ đề xuất cấp độ và báo cáo chủ quản hệ thống thông tin.

b) Đối với hệ thống thông tin được đề xuất là cấp độ 3 hoặc cấp độ 4: đơn vị vận hành trình chủ quản hệ thống thông tin phê duyệt hồ sơ đề xuất cấp độ sau khi có ý kiến thẩm định của đơn vị chức năng theo quy định.

c) Đối với hệ thống thông tin được đề xuất là cấp độ 5: đơn vị vận hành hệ thống thông tin trình chủ quản hệ thống thông tin phê duyệt phương án bảo đảm an toàn thông tin.

Điều 11. Điều chỉnh, bổ sung, thay mới hồ sơ đề xuất cấp độ

Khi thực hiện nâng cấp, mở rộng, thay thế một phần hệ thống thông tin, đơn vị vận hành hệ thống thông tin rà soát phương án bảo đảm an toàn của hệ thống, thực hiện điều chỉnh, bổ sung hoặc thay mới hồ sơ đề xuất cấp độ trong trường hợp cần thiết và trình thẩm định/đánh giá theo quy định.

Chương IV
QUẢN LÝ NGUỒN NHÂN LỰC BẢO ĐẢM AN TOÀN AN NINH MẠNG

Điều 12. Quản lý nguồn nhân lực về an toàn an ninh mạng đối với người dùng là công chức, viên chức, người lao động đang làm việc tại ngành Thuế

1. Tuyển dụng cán bộ vào vị trí công việc về an toàn an ninh mạng:

a) Cán bộ được tuyển dụng vào vị trí công việc về an toàn an ninh mạng phải có bằng tốt nghiệp từ đại học trở lên với các ngành đào tạo về công nghệ thông tin phù hợp với vị trí được tuyển dụng.

b) Vụ Tổ chức cán bộ tổ chức triển khai thực hiện công tác tuyển dụng công chức vào vị trí công việc về an toàn an ninh mạng theo quy định của pháp luật và kế hoạch tuyển dụng của Tổng cục Thuế đã được cấp có thẩm quyền phê duyệt.

2. Trong quá trình làm việc:

a) Công chức, viên chức, người lao động thuộc ngành Thuế phải tuân thủ Quy chế An toàn thông tin mạng và An ninh mạng của ngành Thuế và các quy định khác của đơn vị quản lý.

b) Các đơn vị tổ chức phổ biến, tuyên truyền, đào tạo bồi dưỡng về an toàn an ninh mạng theo quy định tại Điều 8 Quy chế này.

3. Chấm dứt hoặc thay đổi công việc:

a) Công chức, viên chức, người lao động chấm dứt hoặc thay đổi công việc phải được thu hồi: thẻ vào/ra cơ quan (nếu có); thông tin được lưu trên các phương tiện điện tử, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác của cơ quan; quyền truy cập tài nguyên tại vị trí công việc cũ.

b) Đơn vị vận hành thực hiện vô hiệu hóa quyền truy cập tài nguyên, quản trị hệ thống sau khi công chức, viên chức, người lao động thôi việc, nghỉ hưu, chuyển công tác.

c) Công chức, viên chức, người lao động sau khi nghỉ hưu, thôi việc, chuyển công tác phải có cam kết giữ bí mật thông tin bằng văn bản.

Điều 13. Quản lý nguồn nhân lực về an toàn an ninh mạng đối với các đơn vị bên ngoài thực hiện cung cấp các dịch vụ, phần mềm, phần cứng cho ngành Thuế

1. Trước khi làm việc: các đơn vị bên ngoài cung cấp danh sách nhân sự tham gia; nhân sự ký cam kết giữ bí mật thông tin.

2. Trong quá trình làm việc: nhân sự của đơn vị bên ngoài khi làm việc phải tuân thủ các quy định, chính sách về đảm bảo an ninh, an toàn thông tin của đơn vị; có biện pháp bảo vệ đối với các dữ liệu thông tin nhạy cảm, thông tin quan trọng khi trao đổi.

3. Kết thúc quá trình làm việc: đơn vị bên ngoài bàn giao lại tài sản thông tin sử dụng trong quá trình làm việc (nếu có); đơn vị vận hành thực hiện cắt quyền truy cập hệ thống (nếu có), vô hiệu hóa tài khoản đã cung cấp (nếu có).

Chương V
QUẢN LÝ AN TOÀN THÔNG TIN MẠNG TRONG QUẢN LÝ THIẾT KẾ, XÂY DỰNG VÀ VẬN HÀNH HỆ THỐNG THÔNG TIN

Điều 14. Thiết kế an toàn hệ thống thông tin

1. Hệ thống thông tin phải đáp ứng các yêu cầu sau:

a) Sử dụng hệ điều hành, hệ quản trị cơ sở dữ liệu, công cụ phát triển phần mềm có bản quyền hoặc được các cơ quan chức năng đánh giá, xác nhận an toàn; được cung cấp bản vá lỗ hổng, điểm yếu bảo mật trong thời gian hoạt động trên hệ thống mạng.

b) Có thiết kế đáp ứng yêu cầu bảo đảm an toàn hệ thống thông tin theo cấp độ và quy định tại Quy chế này.

c) Khuyến khích áp dụng Khung phát triển phần mềm an toàn theo hướng dẫn của Bộ Thông tin và Truyền thông.

2. Hệ thống thông tin phải bao gồm tối thiểu các tài liệu mô tả:

a) Quy mô, phạm vi và đối tượng sử dụng, khai thác, quản trị, vận hành hệ thống thông tin.

b) Thiết kế và các thành phần của hệ thống thông tin.

c) Phương án bảo đảm an toàn thông tin theo cấp độ.

d) Phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin.

3. Tài liệu về hệ thống thông tin phải được cập nhật trong quá trình vận hành, nâng cấp đảm bảo phản ánh chính xác hiện trạng của hệ thống. Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống.

4. Tài liệu về hệ thống thông tin phải được lưu giữ an toàn, chỉ được cung cấp cho các đối tượng có trách nhiệm đối với hệ thống thông tin.

5. Cục Công nghệ thông tin tổ chức đánh giá hồ sơ thiết kế hệ thống thông tin, các biện pháp bảo đảm an toàn thông tin đối với các hệ thống thông tin trước khi triển khai thực hiện.

6. Thiết kế an toàn hệ thống thông tin phải tuân thủ:

a) Hệ thống thông tin cấp độ 1 tuân thủ quy định tại khoản 1, điểm a và điểm b khoản 2 Điều này;

b) Hệ thống thông tin cấp độ 2, cấp độ 3 tuân thủ quy định tại khoản 1, khoản 2, khoản 3 Điều này;

c) Hệ thống thông tin cấp độ 4 trở lên tuân thủ toàn bộ quy định từ khoản 1 đến khoản 5 Điều này.

Điều 15. Phát triển phần mềm thuê khoán

1. Khi có nhu cầu thuê đơn vị bên ngoài xây dựng phần mềm, đơn vị phát triển phần mềm phải có biên bản, hợp đồng và các cam kết đối với bên thuê khoán các nội dung liên quan đến việc phát triển phần mềm thuê khoán. Trong nội dung hợp đồng phải có điều khoản yêu cầu các đơn vị phát triển phần mềm cung cấp mã nguồn phần mềm.

2. Phần mềm phải được kiểm thử trên môi trường thử nghiệm, kiểm tra, đánh giá an toàn thông tin trước khi đưa vào sử dụng hoặc nâng cấp.

3. Khi thay đổi mã nguồn, kiến trúc phần mềm phải được thực hiện kiểm tra, đánh giá an toàn thông tin cho phần mềm.

4. Đơn vị phát triển phần mềm phải cam kết bảo đảm tính bí mật và bản quyền của phần mềm phát triển.

5. Phần mềm thuê khoán phải đáp ứng các quy định:

a) Hệ thống thông tin cấp độ 2 đáp ứng quy định tại khoản 1 Điều này;

b) Hệ thống thông tin cấp độ 3 đáp ứng quy định tại khoản 1, khoản 2 Điều này;

c) Hệ thống thông tin cấp độ 4 trở lên đáp ứng quy định từ khoản 1 đến khoản 4 Điều này.

Điều 16. Thử nghiệm và nghiệm thu hệ thống

1. Hệ thống thông tin phải thực hiện kiểm thử trước khi đưa vào vận hành, khai thác sử dụng; Việc kiểm thử cần phải xây dựng các nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống trước khi thực hiện.

2. Đơn vị vận hành hệ thống thông tin tổ chức thực hiện thử nghiệm và nghiệm thu hệ thống thông tin do đơn vị vận hành.

3. Đơn vị vận hành hệ thống thông tin thuê đơn vị độc lập (bên thứ 3) hoặc phân công bộ phận độc lập thuộc đơn vị thực hiện giám sát quá trình thử nghiệm và nghiệm thu hệ thống. Trường hợp cần thiết, đơn vị vận hành hệ thống thông tin thành lập Hội đồng giám sát (bao gồm: 01 lãnh đạo thuộc đơn vị làm tổ trưởng và các công chức có chuyên môn nghiệp vụ phù hợp) để thực hiện giám sát quá trình thử nghiệm và nghiệm thu hệ thống.

4. Kết quả thử nghiệm hệ thống thông tin được lập thành Báo cáo nghiệm thu kết quả thử nghiệm gửi các đơn vị tham gia vào quá trình thử nghiệm hệ thống xác nhận. Sau khi các đơn vị tham gia vào quá trình thử nghiệm xác nhận, thủ trưởng đơn vị vận hành hệ thống thông tin trình chủ quản hệ thống thông tin phê duyệt Báo cáo nghiệm thu kết quả thử nghiệm hệ thống thông tin.

5. Hệ thống thông tin phải tuân thủ các nội dung về thử nghiệm và nghiệm thu hệ thống:

a) Hệ thống thông tin cấp độ 1 tuân thủ quy định tại khoản 1 Điều này;

b) Hệ thống thông tin cấp độ 2 tuân thủ quy định tại khoản 1, khoản 2 Điều này;

c) Hệ thống thông tin cấp độ 3 trở lên tuân thủ quy định từ khoản 1 đến khoản 4 Điều này.

Điều 17. Quản lý an toàn mạng

1. Quản lý, vận hành hoạt động của hệ thống:

a) Theo dõi, giám sát hoạt động hàng ngày của hệ thống, kịp thời phát hiện các sự cố bất thường ảnh hưởng đến hệ thống.

b) Thường xuyên cập nhật các bản vá điểm yếu cho hệ điều hành khi có thông báo.

c) Định kỳ 6 tháng/lần rà soát các tài khoản được phép truy cập hệ thống.

2. Trước khi thay đổi cấu hình hệ thống, phải sao lưu dự phòng các tệp tin cấu hình hệ thống và khôi phục hệ thống sau khi xảy ra sự cố.

3. Truy cập và quản lý cấu hình hệ thống:

a) Thiết lập hệ thống chỉ cho phép truy cập quản trị thiết bị từ vùng quản trị. Trường hợp quản trị từ ngoài Internet phải truy cập qua hệ thống VPN hoặc hệ thống truy cập từ xa.

b) Giới hạn địa chỉ được phép truy cập, quản trị thiết bị từ xa.

c) Truy cập thiết bị phải thông qua xác thực người dùng và kết nối có mã hoá.

d) Phân quyền truy cập, quản trị, sử dụng tài nguyên khác nhau trên thiết bị với người sử dụng/ nhóm người sử dụng có chức năng, yêu cầu nghiệp vụ khác nhau (nếu có).

4. Tăng cường bảo mật cho thiết bị trước khi đưa vào vận hành, khai thác: xử lý lỗ hổng, cấu hình tối ưu (cứng hoá).

5. Quản lý an toàn mạng của hệ thống thông tin phải tuân thủ:

a) Hệ thống thông tin cấp độ 1 tuân thủ khoản 1 Điều này;

b) Hệ thống thông tin cấp độ 2 tuân thủ khoản 1, khoản 2 và khoản 3 Điều này;

c) Hệ thống thông tin cấp độ 3 trở lên tuân thủ từ khoản 1 đến khoản 4 Điều này.

Điều 18. Quản lý an toàn máy chủ và ứng dụng

1. Quản lý, vận hành hoạt động của hệ thống máy chủ và dịch vụ:

a) Theo dõi, giám sát hoạt động hàng ngày của hệ thống, kịp thời phát hiện các sự cố bất thường ảnh hưởng đến máy chủ và ứng dụng.

b) Thường xuyên cập nhật các bản vá bảo mật cho hệ điều hành, các phần

mềm cài đặt, các thư viện khi có thông báo.

c) Định kỳ 6 tháng/lần rà soát các tài khoản được phép truy cập máy chủ và ứng dụng.

2. Truy cập mạng của máy chủ: cấu hình, kiểm soát các kết nối, các cổng dịch vụ từ bên trong đi ra cũng như bên ngoài vào máy chủ.

3. Truy cập và quản trị máy chủ và ứng dụng:

a) Thiết lập hệ thống chỉ cho phép truy cập quản trị máy chủ và ứng dụng từ vùng quản trị. Trường hợp quản trị từ ngoài Internet phải truy cập qua hệ thống VPN hoặc hệ thống truy cập từ xa của Tổng cục Thuế.

b) Giới hạn địa chỉ mạng được phép truy cập, quản trị máy chủ từ xa.

c) Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi máy chủ, ứng dụng không nhận được yêu cầu từ người dùng.

d) Thay đổi cổng quản trị mặc định của máy chủ.

e) Phân quyền truy cập, quản trị, sử dụng tài nguyên khác nhau trên máy chủ với người sử dụng/ nhóm người sử dụng có chức năng, yêu cầu nghiệp vụ khác nhau (nếu có).

4. Cập nhật, sao lưu dự phòng cấu hình máy chủ và khôi phục sau khi xảy ra sự cố.

5. Gỡ bỏ các thành phần không còn sử dụng trên hệ điều hành, dịch vụ, phần mềm trên hệ thống máy chủ và ứng dụng.

6. Gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống khi không còn sử dụng.

7. Tăng cường bảo mật cho hệ thống máy chủ trước khi đưa vào vận hành, khai thác: xử lý lỗ hổng, cấu hình tối ưu (cứng hoá).

8. Máy chủ và ứng dụng tuân thủ quy định:

a) Hệ thống thông tin cấp độ 1 tuân thủ quy định tại khoản 1 Điều này;

b) Hệ thống thông tin cấp độ 2 tuân thủ quy định tại khoản 1, khoản 2 Điều này;

c) Hệ thống thông tin cấp độ 3 trở lên tuân thủ quy định từ khoản 1 đến khoản 7 Điều này.

Điều 19. Quản lý an toàn dữ liệu

1. Xác định thông tin quan trọng, thông tin nhạy cảm khi thiết kế hệ thống dựa vào các quy định pháp luật, quy định nghiệp vụ.

2. Sử dụng phương pháp mã hoá theo quy định của pháp luật để mã hoá các thông tin quan trọng, thông tin nhạy cảm.

3. Có phương án an toàn để quản lý và bảo vệ dữ liệu mã hóa, khóa giải mã. Phân quyền truy cập chỉ cho phép người có quyền được truy cập, khai thác

dữ liệu mã hóa.

4. Có phương án kiểm tra tính nguyên vẹn của thông tin quan trọng, thông tin nhạy cảm trong hệ thống (thông qua dữ liệu giấy, dữ liệu có chữ ký số hoặc mã kiểm tra tính nguyên vẹn).

5. Đối với các thông tin nhạy cảm phải thực hiện mã hoá trước khi đưa vào phương tiện lưu trữ, trước khi truyền trên đường truyền (khoá giải mã không gửi kèm dữ liệu đã được mã hoá).

6. Đối với các thông tin mật sử dụng các giải pháp do Ban Cơ yếu quy định (thiết bị lưu trữ ngoài, máy tính, giải pháp mã hoá/giải mã) để truyền nhận. Trường hợp có nhu cầu sử dụng thiết bị lưu trữ ngoài để chứa thông tin mật do Ban Cơ yếu cung cấp, đơn vị có văn bản trực tiếp với Ban Cơ yếu chính phủ (Cục Cơ yếu Đảng Chính quyền) để được cấp theo quy định.

7. Sao lưu định kỳ các dữ liệu, tuỳ thuộc vào tính chất dữ liệu có tần suất sao lưu dự phòng, thời gian lưu trữ tương ứng.

8. Cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống sao lưu dự phòng phụ.

9. Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống, thực hiện sao lưu dự phòng: tập tin cấu hình hệ thống, hệ điều hành máy chủ, hệ quản trị cơ sở dữ liệu, dữ liệu quan trọng khác trên hệ thống (nếu có).

10. Dữ liệu phải được quản lý đảm bảo quy định về an toàn dữ liệu:

a) Hệ thống thông tin cấp độ 1 đảm bảo quy định về phương án sao lưu dự phòng thông tin, dữ liệu, cấu hình hệ thống.

b) Hệ thống thông tin cấp độ 2, cấp độ 3 tuân thủ quy định tại khoản 1, khoản 7 và khoản 9 Điều này.

c) Hệ thống thông tin cấp độ 4 trở lên tuân thủ đầy đủ quy định từ khoản 1 đến khoản 9 Điều này.

Điều 20. Quản lý an toàn thiết bị đầu cuối

1. Quản lý, vận hành hoạt động cho thiết bị đầu cuối (máy tính (máy tính để bàn, máy tính xách tay), máy in, thiết bị phát sóng wifi, thiết bị cầm tay thông minh,...):

a) Theo dõi, giám sát kịp thời phát hiện các sự cố bất thường ảnh hưởng đến thiết bị đầu cuối.

b) Máy tính, thiết bị cầm tay thông minh được cài đặt phần mềm phòng chống mã độc do Tổng cục Thuế cung cấp; cài đặt các phần mềm theo quy định của ngành Thuế; không tự ý cài đặt phần mềm bên ngoài khi chưa được kiểm duyệt bởi Cục Công nghệ thông tin/ Phòng Công nghệ thông tin (trường hợp cần cài đặt thêm phải có ý kiến của lãnh đạo cơ quan).

c) Cập nhật bản vá khi được thông báo hoặc khi phát hiện điểm yếu trên

các thiết bị đầu cuối.

2. Kết nối, truy cập và quản lý cấu hình hệ thống:

a) Nguyên tắc đặt tên máy tính.

- Đối với máy tính cấp cho cá nhân tại Tổng cục Thuế: VPA/VPB-tên tài khoản truy cập *(ví dụ: VPA-NVAN)* và thêm số thứ tự (nếu cần thiết). Trong đó, VPA là tên viết tắt của Cơ quan Tổng cục Thuế, VPB là tên viết tắt của đại diện Văn phòng Tổng cục Thuế tại Tp. HCM.

- Đối với máy tính cấp cho cá nhân tại Cục Thuế: tên viết tắt của Cục Thuế - tên tài khoản truy cập *(ví dụ: HAN-NVAN)* và thêm số thứ tự (nếu cần thiết).

- Đối với máy tính cấp cho cá nhân tại Chi cục Thuế: tên viết tắt của Cục Thuế + tên viết tắt của Chi cục Thuế - tên tài khoản truy cập *(ví dụ: HANTXU-NVAN)* và thêm số thứ tự (nếu cần thiết).

- Đối với máy dùng chung: hoặc Tên viết tắt của đơn vị - chức năng dùng chung (*ví dụ: HAN-DTAO01)*.

b) Không tự ý kết nối thiết bị đầu cuối vào hệ thống mạng nội bộ có dây khi chưa được phê duyệt của cán bộ quản trị mạng. Máy tính phải kết nối với domain ngành Thuế (join domain).

c) Không đăng nhập tài khoản có quyền quản trị trên máy tính (trừ trường hợp phục vụ công tác cài đặt phần mềm mới theo quy định hoặc xử lý lỗi).

d) Khoá máy tính khi rời khỏi nơi đặt máy tính; đặt chế độ cấu hình (sử dụng tính năng của hệ điều hành) khoá màn hình máy tính sau 10 phút nếu không có thao tác của người dùng; tắt máy tính khi rời khỏi cơ quan.

e) Không kết nối với hệ thống mạng không dây, mạng dữ liệu di động (3G/4G/5G...) khi đang kết nối hệ thống mạng có dây; không sử dụng các thiết bị lưu trữ ngoài kết nối qua cổng USB của máy tính (trừ các trường hợp phục vụ công tác xử lý lỗi máy tính, sử dụng thiết bị lưu trữ mật do Ban Cơ yếu Chính phủ cung cấp).

f) Căn cứ yêu cầu về bảo đảm an toàn thông tin mạng, Cục Công nghệ thông tin có thể hướng dẫn cài đặt thêm phần mềm giám sát an toàn thông tin mạng.

3. Quản lý và sử dụng máy tính soạn thảo văn bản chứa nội dung bí mật nhà nước:

a) Sử dụng hệ điều hành và các phần mềm soạn thảo văn bản có bản quyền; không kết nối vào mạng Internet, hệ thống mạng nội bộ, mạng dữ liệu di động, trừ trường hợp đã áp dụng các biện pháp bảo vệ theo hướng dẫn của Ban Cơ yếu Chính phủ; chỉ sử dụng thiết bị lưu trữ mật do Ban Cơ yếu Chính phủ cung cấp.

b) Phân quyền truy cập máy tính theo tên người hoặc đơn vị cấp vụ/phòng/đội được giao soạn thảo bí mật nhà nước.

c) Trường hợp ổ cứng lỗi cần bảo hành, phải thực hiện biện pháp xóa toàn

bộ dữ liệu trước khi mang ổ cứng ra khỏi cơ quan và có biên bản ghi nhận về việc xóa dữ liệu giữa đơn vị sử dụng máy tính và đơn vị nhận ổ cứng. Việc sửa chữa, nâng cấp phần mềm cho máy tính (sau khi đã đưa vào sử dụng), nếu yêu cầu phải tiếp cận các tệp tin trên ổ cứng, thực hiện dưới sự giám sát của đơn vị sử dụng máy tính, đảm bảo không lộ lọt dữ liệu trên ổ cứng máy tính ra bên ngoài (có biên bản giữa đơn vị sử dụng máy tính và đơn vị sửa chữa, nâng cấp phần mềm).

4. Cài đặt, kết nối, bảo hành và gỡ bỏ thiết bị đầu cuối trong hệ thống:

a) Khi không còn nhu cầu sử dụng các thiết bị đầu cuối (không phải là máy tính) phải được xoá bỏ cấu hình, dữ liệu trước khi làm thủ tục thu hồi.

b) Máy tính khi được chuyển sử dụng từ cá nhân này sang cá nhân khác, không tiếp tục sử dụng cho công việc của cơ quan, máy tính khi mang đi bảo hành, bảo dưỡng, sửa chữa có ổ cứng thì phải thực hiện xóa toàn bộ dữ liệu trên ổ cứng.

5. Cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho máy tính người sử dụng trước khi đưa hệ thống vào sử dụng.

6. Kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin cho thiết bị đầu cuối trước khi đưa vào sử dụng.

Điều 21. Quản lý phòng chống phần mềm độc hại

1. Máy tính, máy chủ (trừ máy tính mật, các máy chủ cài đặt hệ điều hành đóng do hãng cung cấp) và các thiết bị di động (nếu có) phải được cài đặt phần mềm phòng chống mã độc do Tổng cục Thuế cung cấp. Cấu hình đảm bảo các thiết bị cập nhật tự động các bản nâng cấp từ hệ thống tập trung. Riêng các máy tính ngoài trụ sở cơ quan thuế, trường hợp không cập nhật được tự động thì định kỳ hàng tuần máy tính phải được cập nhật thủ công các bản nâng cấp mới nhất.

2. Việc cài đặt các phần mềm theo quy định tại điểm b khoản 1 Điều 20 của Quy chế này. Các phần mềm trước khi cài đặt trên máy tính đều phải được kiểm tra bằng phần mềm phòng chống mã độc.

3. Các file trao đổi qua môi trường mạng như qua email, qua chat, từ website và qua các phương tiện lưu trữ (trường hợp được sử dụng) phải được rà quét trước khi lưu vào máy tính.

4. Định kỳ thực hiện dò quét phần mềm độc hại trên toàn bộ thiết bị (máy tính theo tuần, máy chủ theo tháng) từ hệ thống quản lý phần mềm phòng chống mã độc; phân công công chức làm công nghệ thông tin hàng ngày (ngày làm việc) vào hệ thống quản lý phần mềm phòng chống mã độc để kiểm tra hoạt động hệ thống, kịp thời phát hiện và xử lý các máy tính có dấu hiệu nhiễm mã độc.

Điều 22. Quản lý giám sát an toàn hệ thống thông tin

1. Quản lý, vận hành hoạt động của hệ thống giám sát:

a) Hệ thống giám sát tập trung do Tổng cục Thuế triển khai được theo dõi, giám sát kịp thời phát hiện các sự cố bất thường ảnh hưởng đến hệ thống giám sát.

b) Thường xuyên cập nhật các bản vá bảo mật cho hệ thống giám sát khi có thông báo.

c) Định kỳ 6 tháng/lần rà soát các tài khoản được phép truy cập hệ thống giám sát.

2. Đối tượng giám sát tối thiểu: máy chủ, ứng dụng, dịch vụ và các thành phần khác của các hệ thống thông tin từ cấp độ 3 trở lên; thiết bị hạ tầng truyền thông, thiết bị bảo mật tại Cục Thuế.

3. Các đối tượng giám sát phải được cấu hình gửi nhật ký về hệ thống giám sát trước khi chính thức đưa vào hoạt động.

4. Thiết lập chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị hệ thống giám sát; giới hạn địa chỉ mạng được phép truy cập, quản trị hệ thống giám sát từ xa.

5. Thông tin giám sát gồm tối thiểu các thông tin truy cập, thông tin thay đổi cấu hình (nếu có), thông tin các log cảnh báo.

6. Thông tin giám sát phải được lưu trữ và phân quyền truy cập.

7. Hệ thống giám sát và thiết bị được giám sát phải được đồng bộ thời gian với máy chủ thời gian của Tổng cục Thuế.

8. Tổ chức thực hiện theo dõi, giám sát và cảnh báo sự cố, hoạt động của hệ thống giám sát 24 giờ/ngày và 7 ngày/tuần.

Điều 23. Quản lý điểm yếu an toàn thông tin

1. Đơn vị vận hành có trách nhiệm quản lý thông tin các thành phần có trong hệ thống có khả năng tồn tại điểm yếu an toàn thông tin, bao gồm: thiết bị mạng, thiết bị bảo mật, hệ điều hành, máy chủ, các phần mềm cài đặt trên máy chủ, ứng dụng, dịch vụ và các thành phần khác (nếu có).

2. Bộ phận chuyên trách an toàn an ninh mạng thường xuyên cập nhật các điểm yếu an toàn thông tin từ Bộ Thông tin và Truyền thông (Cục An toàn thông tin); Bộ Công an (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao; Cục Kỹ thuật nghiệp vụ); Bộ Quốc phòng (Ban Cơ yếu Chính phủ; Bộ Tư lệnh tác chiến không gian mạng); Bộ Tài chính (Cục Tin học và Thống kê tài chính); Tổng cục Thuế (Cục Công nghệ thông tin); đơn vị cung cấp dịch vụ giám sát an toàn thông tin mạng cho Tổng cục Thuế; đơn vị cung cấp dịch vụ kiểm tra, đánh giá an toàn thông tin mạng cho Tổng cục Thuế; đơn vị cung cấp sản phẩm; nhà sản xuất các sản phẩm phần cứng, phần mềm đang sử dụng tại Tổng cục Thuế. Bộ phận chuyên trách an toàn an ninh mạng thực hiện đánh giá, phân loại và thông báo cho các đơn vị vận hành.

3. Khi tiếp nhận thông tin về điểm yếu an toàn thông tin, đơn vị vận hành

phối hợp các đơn vị liên quan (đơn vị cung cấp dịch vụ, đơn vị cung cấp sản phẩm,..) qua email, điện thoại (nếu cần) để phân tích, lên kế hoạch và xử lý các điểm yếu. Các điểm yếu an toàn thông tin chưa thể xử lý ngay, đơn vị vận hành phối hợp cùng Phòng An toàn thông tin - Cục Công nghệ thông tin có phương án xử lý tạm thời cho các điểm yếu an toàn thông tin.

4. Các hệ thống thông tin trước khi đưa vào sử dụng phải được Cục Công nghệ thông tin (Phòng An toàn thông tin) đánh giá điểm yếu. Đồng thời, định kỳ đánh giá điểm yếu an toàn thông tin cho các hệ thống thông tin theo quy định tại khoản 2 Điều 6 của Quy chế này.

Điều 24. Quản lý sự cố an toàn thông tin

1. Đơn vị vận hành hệ thống thông tin:

a) Xây dựng và phê duyệt kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng; phương án ứng phó, khắc phục sự cố an ninh mạng cho các hệ thống thông tin thuộc quản lý vận hành của đơn vị theo đề cương tại Phụ lục II Quyết định số 05/2017/QĐ-TTg (đối với hệ thống cấp độ 4, 5); phụ lục III ban hành kèm theo Thông tư số 20/2017/TT-BTTTT (đối với hệ thống cấp độ 1, 2, 3) và quy định tại Điều 25 của Nghị định số 53/2022/NĐ-CP.

b) Tổ chức triển khai kế hoạch và phương án ứng phó, khắc phục sự cố an ninh mạng.

c) Đối với hệ thống thông tin quan trọng về an ninh Quốc gia: đơn vị vận hành hệ thống thông tin thực hiện theo quy định tại khoản 2 Điều 10 Quy chế An toàn thông tin mạng và An ninh mạng Bộ Tài chính ban hành kèm theo Quyết định số 1013/QĐ-BTC ngày 19/5/2023 của Bộ trưởng Bộ Tài chính.

2. Cục Công nghệ thông tin:

a) Theo dõi trên phương tiện thông tin đại chúng và mạng Internet, qua các cơ quan chức năng, qua hệ thống giám sát được quy định tại Điều 22 của Quy chế này về các sự kiện mất an toàn thông tin mạng có thể tác động tới Tổng cục Thuế.

b) Hướng dẫn các đơn vị kiểm tra, rà soát trong nội bộ đơn vị theo các văn bản cảnh báo, hướng dẫn của các cơ quan chức năng và các tổ chức về an toàn thông tin.

c) Thiết lập kênh trao đổi thông tin (qua email, điện thoại) với các đối tác cung cấp thiết bị, phần mềm, giải pháp an toàn thông tin để kịp thời thông báo và phối hợp xử lý các sự cố tác động tới hệ thống thông tin.

3. Khi có sự cố về an toàn thông tin mạng, Cục Công nghệ thông tin có trách nhiệm phối hợp ngay với cơ quan chức năng, các nhóm chuyên gia, các đơn vị cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin.

4. Sau khi xảy ra sự cố, đơn vị vận hành hệ thống thông tin thực hiện báo cáo theo quy định tại Điều 11 Quyết định số 05/2017/QĐ-TTg và Điều 9 Thông

tư 20/2017/TT-BTTTT đồng thời trình Tổng cục Thuế (qua Cục Công nghệ thông tin) báo cáo Bộ Tài chính (qua Cục Tin học và Thống kê tài chính).

5. Định kỳ hàng năm, Cục Công nghệ thông tin trình Tổng cục tổ chức diễn tập ứng cứu sự cố theo kế hoạch và phương án ứng phó, khắc phục sự cố an toàn thông tin mạng đã được phê duyệt trong phạm vi các hệ thống thông tin do Tổng cục Thuế làm chủ quản; tham gia các cuộc diễn tập Quốc gia, Quốc tế do Cơ quan điều phối Quốc gia hoặc các cơ quan chức năng thuộc Bộ Thông tin và Truyền thông, Bộ Công an, Bộ Quốc phòng tổ chức.

6. Cục Công nghệ thông tin đăng ký tham gia Mạng lưới ứng cứu sự cố an toàn thông tin mạng Quốc gia theo quy định tại khoản 2 Điều 7 Quyết định số 05/2017/QĐ-TTg.

Điều 25. Quản lý an toàn người sử dụng

1. Quản lý truy cập, sử dụng tài nguyên nội bộ:

a) Người sử dụng khi truy cập, sử dụng tài nguyên nội bộ phải đăng ký và được phân quyền chặt chẽ; không đăng nhập máy tính bằng tài khoản quản trị trừ trường hợp chuyên viên công nghệ thông tin đăng nhập để thực hiện công việc chuyên môn; máy tính truy cập, sử dụng tài nguyên nội bộ phải đáp ứng quy định tại Điều 20 của Quy chế này. Trường hợp truy cập từ bên ngoài mạng nội bộ hoặc từ máy tính không đảm bảo quy định tại Điều 20 của Quy chế này, người sử dụng phải thông qua hệ thống truy cập từ xa do Tổng cục Thuế triển khai.

b) Đảm bảo văn bản quyết định về tiếp nhận, bổ nhiệm, điều động, chuyển đổi công tác gửi tới Cục Công nghệ thông tin/Phòng Công nghệ thông tin/bộ phận công nghệ thông tin tại thời điểm phát hành văn bản; kịp thời điều chỉnh phân quyền, thu hồi quyền truy cập sử dụng tài nguyên nội bộ khi người sử dụng thay đổi vị trí công tác hoặc chuyển công tác, nghỉ việc.

c) Không lưu thông tin ngoài phạm vi công việc và hoạt động của cơ quan trên ổ đĩa mạng, chia sẻ thông tin trên ổ đĩa mạng đúng phạm vi cần chia sẻ, xóa thông tin trên ổ đĩa mạng do bản thân tạo ra sau khi thông tin hết giá trị sử dụng.

d) Nghiêm cấm sử dụng địa chỉ thư điện tử công vụ để đăng ký sử dụng các ứng dụng, dịch vụ ngoài phạm vi công việc. Không mở các địa chỉ trong nội dung thư, mở tệp đính kèm hoặc thực hiện theo hướng dẫn của thư điện tử có địa chỉ nhận không rõ nguồn gốc. Không truy cập các hệ thống thông tin cung cấp cho cán bộ thuế sử dụng từ bên ngoài mạng nội bộ (email, hệ thống thông tin nhật ký thanh tra kiểm tra, hệ thống thông tin văn bản điện tử,...) bằng các máy tính không đảm bảo an toàn bảo mật. Khi phát hiện thư điện tử nhận được là thư rác, thư giả mạo, người dùng cần thông báo cho bộ phận hỗ trợ kỹ thuật của Cục Công nghệ thông tin/ Phòng Công nghệ thông tin để áp dụng biện pháp ngăn chặn.

e) Đặt mật khẩu các tệp tin có nội dung nhạy cảm trước khi gửi qua thư điện tử hoặc đưa vào thiết bị lưu trữ. Gửi mật khẩu cho người nhận bằng phương

thức khác không kèm với tệp tin.

f) Không sử dụng các công cụ tự xây dựng để cập nhật dữ liệu vào các hệ thống thông tin do Bộ Tài chính, Tổng cục Thuế xây dựng và triển khai. Trường hợp công cụ tự xây dựng phục vụ nhu cầu khai thác dữ liệu thì phải đảm bảo yêu cầu về an toàn thông tin mạng và được phê duyệt hồ sơ cấp độ khi đưa vào sử dụng.

g) Không được lắp đặt các thiết bị tự trang bị (thiết bị mạng, thiết bị viễn thông (4G), thiết bị đầu cuối (máy in, Ip phone), ...) vào hệ thống mạng nội bộ của cơ quan.

2. Tài khoản người dùng phải tuân thủ quy định tại Điều 26 của Quy chế này; đổi mật khẩu tài khoản người dùng trong trường hợp phát hiện mật khẩu bị lộ lọt thông tin.

3. Phối hợp với Cục Công nghệ thông tin/Phòng Công nghệ thông tin trong việc triển khai các biện pháp an toàn thông tin mạng trên máy tính của người dùng, gỡ mã độc (nếu phát hiện có mã độc mà phần mềm phòng diệt mã độc không có khả năng xử lý), xác định nguyên nhân mất an toàn thông tin mạng liên quan đến người dùng hoặc máy tính của người dùng.

Điều 26. Quản lý an toàn tài khoản thông tin

1. Tài khoản thông tin là tập hợp gồm tên đăng nhập và mật khẩu hoặc hình thức xác thực khác, được gắn với quyền truy cập thực hiện một số tác vụ trên hệ thống thông tin hoặc trên thiết bị xử lý thông tin, bao gồm các loại sau:

a) Tài khoản định danh: là tài khoản cấp cho một người dùng duy nhất và được gắn quyền truy cập các hệ thống thông tin mà người dùng đó được sử dụng trừ các tài khoản sử dụng vào mục đích chung không gây ảnh hưởng đến việc cài đặt, cấu hình hệ thống, ứng dụng.

b) Tài khoản nhiệm vụ dùng để truy cập hệ thống gắn với một nhiệm vụ cụ thể để thực hiện nhiệm vụ của cơ quan (ví dụ: tài khoản văn thư, tài khoản biên tập, tài khoản vận hành, tài khoản backup...). Tài khoản này phải được bàn giao cho công chức, viên chức, người lao động cụ thể quản lý. Khi kết thúc thời gian thực hiện nhiệm vụ, người dùng bàn giao tài khoản nhiệm vụ cho người dùng được phân công tiếp nhận nhiệm vụ hoặc bàn giao tài khoản cho đơn vị quản lý người dùng.

c) Tài khoản hệ thống là tài khoản gắn với một ứng dụng cụ thể để thực hiện xác thực giữa các ứng dụng hoặc ứng dụng với cơ sở dữ liệu.

d) Tài khoản quản trị gắn với quyền cài đặt, cấu hình các thông số và cấp quyền truy cập trên hệ thống thông tin gồm: quản trị nội dung, quản trị ứng dụng, quản trị cơ sở dữ liệu, quản trị hệ điều hành, quản trị thiết bị. Tài khoản quản trị được giao cho cá nhân, đơn vị thực hiện nhiệm vụ quản trị ứng dụng, quản trị cơ sở dữ liệu, quản trị hệ điều hành, quản trị thiết bị. Trường hợp thuê

dịch vụ quản trị hệ thống, đơn vị chủ trì thuê dịch vụ phải quản lý việc sử dụng tài khoản quản trị của đơn vị cung cấp dịch vụ: lập danh sách cá nhân được giao tài khoản quản trị, thời điểm cá nhân tiếp nhận tài khoản, thời điểm kết thúc sử dụng; cập nhật danh sách khi có thay đổi về nhân sự giữ tài khoản.

2. Quy định về tài khoản:

a) Các tài khoản (trừ tài khoản hệ thống) phải được Lãnh đạo đơn vị phê duyệt.

b) Cá nhân được cấp hoặc giao quản lý tài khoản chịu trách nhiệm về các hành vi của tài khoản được ghi nhận trên thiết bị xử lý thông tin, hệ thống thông tin, hệ thống giám sát an toàn thông tin mạng.

c) Tài khoản (trừ tài khoản hệ thống) nếu đăng nhập quá 5 lần sẽ bị tạm khoá trong thời gian 5 phút.

d) Tài khoản nếu không sử dụng trong 03 tháng sẽ bị tạm khoá.

e) Định kỳ 6 tháng/lần đơn vị vận hành kiểm tra loại bỏ các tài khoản không sử dụng, các tài khoản không còn hợp lệ trên hệ thống thông tin.

3. Quy định về mật khẩu của tài khoản thông tin:

a) Mật khẩu phải đáp ứng các yêu cầu sau: Có tối thiểu 8 ký tự, gồm tối thiểu 3 trong 4 loại ký tự sau: chữ cái viết hoa (A - Z), chữ cái viết thường (a - z), chữ số (0 - 9), các ký tự; mật khẩu không chứa tên tài khoản.

b) Mật khẩu phải được giữ bí mật và được đổi ngay sau khi tài khoản được bàn giao giữa các cá nhân, đơn vị hoặc khi nghi ngờ bị lộ. Mật khẩu phải được thay đổi ít nhất một lần trong 06 tháng (trừ tài khoản hệ thống).

c) Mật khẩu của tài khoản quản trị do hệ thống sinh ra (administrator/root/...) phải được đóng phong bì bàn giao cho Lãnh đạo Cục Công nghệ thông tin (tại Tổng cục Thuế), Lãnh đạo Phòng Công nghệ thông tin (tại Cục Thuế), Lãnh đạo đội phụ trách bộ phận Công nghệ thông tin (tại Chi cục Thuế).

3. Quy định về xác thực đa nhân tố:

a) Khuyến khích sử dụng xác thực tối thiểu 2 yếu tố để tăng cường an toàn bảo mật.

b) Các hệ thống cho phép truy cập từ Internet đối với người dùng công chức, viên chức ngành Thuế, người dùng là cán bộ quản trị, cán bộ hỗ trợ bắt buộc sử dụng tối thiểu 2 yếu tố.

c) Đối với các hệ thống khác tuỳ thuộc vào tính chất quan trọng, giao Cục trưởng Cục Công nghệ thông tin quyết định.

Điều 27. Quản lý an toàn kết nối Internet

1. Người dùng khi truy cập sử dụng Internet từ máy tính có kết nối mạng nội bộ phải thông qua hệ thống Internet an toàn do Tổng cục Thuế triển khai.

Trường hợp máy tính xách tay (không kết nối mạng nội bộ), máy tính đặt ngoài trụ sở kết nối Internet thông qua mạng không dây (wifi), mạng dữ liệu di động (3G/4G/5G...) chỉ vào các trang Website phục vụ công việc.

2. Đối với hệ thống máy chủ, thiết bị mạng, bảo mật khi kết nối ra ngoài Internet để cập nhật (bản vá, các thông tin từ hãng) ưu tiên cập nhật qua hệ thống truy cập Internet do Tổng cục Thuế triển khai. Trường hợp hệ thống máy chủ, thiết bị mạng, bảo mật không hỗ trợ kết nối ra ngoài Internet qua hệ thống truy cập Internet do Tổng cục Thuế triển khai, các thiết bị trên có thể cập nhật trực tiếp từ Internet nhưng phải có khai báo địa chỉ cụ thể để thiết lập chính sách trên tường lửa.

3. Cục Công nghệ thông tin công bố và quản lý danh sách địa chỉ trang web Internet được phép truy cập. Trường hợp đơn vị có yêu cầu truy cập trang web không nằm trong danh sách địa chỉ trang web Internet đã công bố, thủ trưởng đơn vị gửi văn bản đề nghị về Cục Công nghệ thông tin.

Điều 28. Quản lý an toàn khi kết thúc sử dụng hệ thống thông tin

1. Hệ thống thông tin phải kết thúc sử dụng khi đã được thay thế hoàn toàn bằng hệ thống thông tin khác hoặc không còn giá trị sử dụng.

2. Thành phần của hệ thống thông tin phải kết thúc sử dụng khi đã hết thời gian khấu hao sử dụng theo quy định pháp luật về quản lý, sử dụng tài sản công và được cấp có thẩm quyền cho phép dừng sử dụng.

3. Thủ tục kết thúc vận hành, khai thác, hủy bỏ hệ thống thông tin:

a) Đơn vị vận hành hệ thống thông tin báo cáo chủ quản hệ thống thông tin cho phép kết thúc vận hành, khai thác hệ thống thông tin.

b) Đơn vị vận hành xóa bỏ nội dung thông tin, thông tin cấu hình dữ liệu trên thiết bị vật lý trước khi chuyển sang bộ phận quản lý tài sản chờ thanh lý.

Chương VI
TỔ CHỨC THỰC HIỆN

Điều 29. Trách nhiệm của các cơ quan, đơn vị thuộc ngành Thuế

1. Cục Công nghệ thông tin:

a) Tham mưu cho Lãnh đạo Tổng cục Thuế về việc triển khai công tác an toàn an ninh mạng; hướng dẫn các quy định của pháp luật, văn bản chỉ đạo và hướng dẫn của các cơ quan có thẩm quyền về an toàn an ninh mạng trong phạm vi các cơ quan, đơn vị, tổ chức thuộc ngành Thuế; tổ chức triển khai Quy chế này và các quy định của pháp luật về an toàn an ninh mạng tại Tổng cục Thuế, Cục Thuế.

b) Tổng hợp kế hoạch, báo cáo định kỳ, đột xuất về an toàn an ninh mạng,

trình Lãnh đạo Tổng cục Thuế gửi các cơ quan quản lý về an toàn an ninh mạng; xử lý các việc đột xuất về an toàn an ninh mạng theo phân công của Tổng cục Thuế.

c) Định kỳ hàng năm hoặc khi có thay đổi trong quy định của Nhà nước, chỉ đạo của cấp có thẩm quyền về an toàn an ninh mạng: tổ chức rà soát, kiểm tra tính phù hợp của Quy chế này với các quy định của pháp luật về an toàn an ninh mạng; kiểm tra tính đáp ứng của Quy chế này với yêu cầu thực tế của Tổng cục Thuế; báo cáo Tổng cục về việc sửa đổi, bổ sung Quy chế trong trường hợp cần thiết; lập hồ sơ lưu thông tin phản hồi của đối tượng áp dụng Quy chế về an toàn an ninh mạng của Tổng cục Thuế làm căn cứ xây dựng đề xuất cập nhật, bổ sung Quy chế.

2. Cục Thuế:

a) Tổ chức tuyên truyền, triển khai thực hiện Quy chế này và các quy định của pháp luật, văn bản chỉ đạo và hướng dẫn của các cơ quan có thẩm quyền về an toàn an ninh mạng trong phạm vi đơn vị; xây dựng kế hoạch, báo cáo định kỳ, đột xuất về an toàn an ninh mạng và gửi Cục Công nghệ thông tin tổng hợp, báo cáo Tổng cục.

b) Chỉ đạo Phòng Công nghệ thông tin phối hợp chặt chẽ với Phòng An toàn thông tin - Cục Công nghệ thông tin trong quá trình triển khai công tác an toàn an ninh mạng tại đơn vị.

c) Ban hành quy định/ nội quy về an toàn an ninh mạng của đơn vị phù hợp với trách nhiệm của đơn vị theo Quy chế này và các quy định của pháp luật về an toàn an ninh mạng (nếu cần).

3. Chi cục Thuế:

a) Tổ chức tuyên truyền, triển khai thực hiện Quy chế này và các quy định của pháp luật, văn bản chỉ đạo và hướng dẫn của các cơ quan có thẩm quyền về an toàn an ninh mạng trong phạm vi đơn vị; xây dựng kế hoạch, báo cáo định kỳ, đột xuất về an toàn an ninh mạng và gửi Phòng Công nghệ thông tin Cục Thuế.

b) Chỉ đạo bộ phận công nghệ thông tin phối hợp chặt chẽ với Phòng Công nghệ thông tin - Cục Thuế trong quá trình triển khai công tác an toàn an ninh mạng tại đơn vị.

c) Ban hành quy định/ nội quy về an toàn an ninh mạng của đơn vị phù hợp với trách nhiệm của đơn vị theo Quy chế này và các quy định của pháp luật về an toàn an ninh mạng (nếu cần).

4. Các đơn vị thuộc và trực thuộc Tổng cục Thuế:

a) Phối hợp với Cục Công nghệ thông tin triển khai và giám sát việc thực hiện Quy chế này tại đơn vị.

b) Vụ Tuyên truyền - Hỗ trợ người nộp thuế và Văn phòng phối hợp tổ

chức tuyên truyền an toàn an ninh mạng cho công chức, viên chức, người lao động thuộc cơ quan Tổng cục Thuế; an toàn an ninh mạng cho người nộp thuế.

Điều 30. Trách nhiệm cá nhân thuộc Tổng cục Thuế

1. Thủ trưởng đơn vị thuộc đối tượng áp dụng của Quy chế này có trách nhiệm: phổ biến, quán triệt tới từng công chức, viên chức, người lao động của đơn vị thuộc phạm vi quản lý thực hiện nghiêm các quy định của pháp luật, quy định của Bộ Tài chính, quy định của ngành Thuế về an toàn an ninh mạng, bảo vệ dữ liệu cá nhân, bảo vệ bí mật nhà nước trên không gian mạng; thường xuyên kiểm tra việc thực hiện Quy chế này tại đơn vị; chịu trách nhiệm trước pháp luật và Lãnh đạo Tổng cục Thuế 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 cán bộ của đơn vị thực hiện đúng quy định hoặc để hệ thống thông tin thuộc phạm vi quản lý không đảm bảo các quy định về an toàn thông tin mạng.

2. Công chức, viên chức, người lao động thuộc ngành Thuế có trách nhiệm: tuân thủ Quy chế; thông báo các vấn đề bất thường liên quan tới an toàn an ninh mạng cho đơn vị chuyên trách an toàn an ninh mạng; 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 chế.

3. Cá nhân vi phạm Quy chế này làm ảnh hưởng đến việc thực hiện nhiệm vụ chính trị của Tổng cục Thuế hoặc gây phương hại đến an ninh Quốc gia thì tùy theo tính chất, mức độ của hành vi vi phạm sẽ bị xử lý hành chính, xử lý kỷ luật hoặc truy cứu trách nhiệm hình sự. Nếu gây thiệt hại về tài sản thì phải bồi thường theo quy định của pháp luật.

Điều 31. Điều khoản chuyển tiếp

Cục Công nghệ thông tin, Cục Thuế, Chi cục Thuế xây dựng, hoàn thiện hồ sơ cấp độ, tổ chức thẩm định (hoặc lấy ý kiến thẩm định) và trình cấp có thẩm quyền phê duyệt, điều chỉnh, bổ sung hồ sơ đề xuất cấp độ chưa đáp ứng các quy định của Thông tư số 12/2022/TT-BTTTT và Quy chế này.

Điều 32. Tổ chức thực hiện

1. Cục Công nghệ thông tin chịu trách nhiệm hướng dẫn, theo dõi, kiểm tra, đôn đốc việc thực hiện Quy chế này.

2. Các đơn vị vận hành thực hiện xây dựng kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng, phương án ứng phó, khắc phục sự cố an ninh mạng trước quý 1 năm 2025.

3. Trong quá trình thực hiện Quy chế này, nếu phát sinh khó khăn, vướng mắc, các đơn vị, cá nhân gửi ý kiến về Cục Công nghệ thông tin để tổng hợp, báo cáo, đề xuất trình Lãnh đạo Tổng cục xem xét, quyết định./.