Ký bởi: BỘ TÀI CHÍNH
Cơ quan: 28 Trần Hưng Đạo
Thời gian ký: 22/05/2023 16:44:45 +07:00

BỘ TÀI CHÍNH	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
	Độc lập - Tự do – Hạnh phúc
Số: 1013 /QĐ-BTC	*Hà Nội, ngày 19 tháng 5 năm 2023*

QUYẾT ĐỊNH
Ban hành Quy chế An toàn thông tin mạng và An ninh mạng Bộ Tài chính

BỘ TRƯỞNG BỘ TÀI CHÍNH

Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19/11/2015;

Căn cứ Luật An ninh mạng số 24/2018/QH14 ngày 12/6/2018;

Căn cứ Luật Bảo vệ bí mật nhà nước số 29/2018/QH14 ngày 15/11/2018;

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 Nghị định số 14/2023/NĐ-CP ngày 20/4/2023 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của 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;

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

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế An toàn thông tin mạng và An ninh mạng Bộ Tài chính.

Điều 2. Quyết định này có hiệu lực từ ngày ký, thay thế Quyết định số 201/QĐ-BTC ngày 12/02/2018 của Bộ trưởng Bộ Tài chính về việc ban hành Quy chế An toàn thông tin mạng Bộ Tài chính.

Điều 3. Cục trưởng Cục Tin học và Thống kê tài chính, Thủ trưởng các tổ chức hành chính, sự nghiệp thuộc cơ cấu tổ chức của Bộ Tài chính; các đơn vị và cá nhân thuộc Bộ Tài chính có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Bộ Thông tin và Truyền thông;
- Bộ Công an;
- Bộ Quốc phòng;
- Cổng thông tin điện tử Bộ Tài chính;
- Lưu: VT, THTK.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

BỘ TÀI CHÍNH

Nguyễn Đức Chi

BỘ TÀI CHÍNH	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 Bộ Tài chính
(Kèm theo Quyết định số 1013/QĐ-BTC ngày 19 tháng 5 năm 2023 của Bộ Tài chính)

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 Bộ Tài chính.

2. Quy chế này áp dụng với các tổ chức hành chính, sự nghiệp thuộc cơ cấu tổ chức của Bộ Tài chính (theo Nghị định số 14/2023/NĐ-CP ngày 20/4/2023 của Chính phủ quy định về chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Tài chính).

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. *Mạng* là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua mạng viễn thông và mạng máy tính.

5. *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.

6. *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).

7. *Người dùng* là cán bộ, công chức, viên chức, người lao động tại các đơn vị thuộc Bộ Tài chính sử dụng máy tính để xử lý công việc.

8. *Tổng cục* là đơn vị cấp Tổng cục hoặc tương đương thuộc Bộ Tài chính (Tổng cục Thuế, Tổng cục Hải quan, Tổng cục Dự trữ Nhà nước, Kho bạc Nhà nước, Ủy ban Chứng khoán Nhà nước).

9. *Cơ quan Bộ* là bao gồm các tổ chức cấp Vụ, Cục và tương đương trực thuộc Bộ Tài chính và các tổ chức, đơn vị sử dụng hệ thống mạng nội bộ tại trụ sở Bộ Tài chính tại Hà Nội và trụ sở Đại diện Văn phòng Bộ Tài chính tại Thành phố Hồ Chí Minh.

Điều 3. Nguyên tắc an toàn an ninh mạng tại Bộ Tài chính

1. Tuân thủ quy định của pháp luật về an toàn thông tin mạng, 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.

2. 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 Bộ Tài chính.

3. An toàn an ninh mạng phải gắn liền và hỗ trợ các hoạt động ứng dụng công nghệ thông tin, giao dịch điện tử, chuyển đổi số của Bộ Tài chính; hỗ trợ việc sử dụng thiết bị xử lý thông tin để xử lý công việc của cán bộ, công chức, viên chức, người lao động thuộc Bộ Tài chính.

4. Ứng cứu sự cố an toàn an ninh mạng là hoạt động quan trọng nhằm phát hiện, ngăn chặn, xử lý và khắc phục kịp thời sự cố an toàn an ninh mạng.

5. Mỗi cán bộ, công chức, viên chức, người lao động tại các đơn vị thuộc Bộ Tài chính nêu cao tinh thần chủ động, tự giác trong việc áp dụng các biện pháp an toàn an ninh mạng.

Chương II
PHÂN CÔNG NHIỆM VỤ AN TOÀN AN NINH MẠNG

Điều 4. Phân công thực hiện các vai trò về bảo đảm an toàn thông tin mạng, an ninh mạng theo quy định của pháp luật

1. Chủ quản hệ thống thông tin:

a) Bộ Tài chính là chủ quản của hệ thống thông tin được xây dựng, thiết lập, nâng cấp, mở rộng từ dự án hoặc kế hoạch thuê dịch vụ thuộc thẩm quyền phê duyệt của Bộ trưởng Bộ Tài chính; chủ quản của hệ thống thông tin được xây dựng, thiết lập, nâng cấp, mở rộng từ dự án, kế hoạch thuê dịch vụ, đề cương và dự toán chi tiết thuộc thẩm quyền phê duyệt của đơn vị thuộc Cơ quan Bộ, đơn vị sự nghiệp trực thuộc Bộ.

Bộ Tài chính ủy quyền cho Tổng cục thực hiện trách nhiệm của chủ quản hệ thống thông tin đối với hệ thống thông tin do Tổng cục làm chủ đầu tư dự án, chủ trì thực hiện kế hoạch thuê dịch vụ. Đơn vị được ủy quyền chủ quản hệ thống thông tin thực hiện đầy đủ trách nhiệm của chủ quản hệ thống thông tin theo quy định của pháp luật về an toàn an ninh mạng và quy định tại Quy chế này. Việc ủy quyền được kết thúc tại thời điểm hệ thống thông tin được Bộ Tài chính phê duyệt kết thúc sử dụng hoặc được Bộ Tài chính chuyển giao trách nhiệm chủ quản cho đơn vị khác theo quy định hiện hành. Phạm vi của hệ thống thông tin được ủy quyền quy định tại quyết định phê duyệt đầu tư dự án; kế hoạch thuê dịch vụ công nghệ thông tin; đề cương và dự toán chi tiết.

b) Tổng cục là chủ quản của hệ thống thông tin được xây dựng, thiết lập, nâng cấp, mở rộng từ dự án, kế hoạch thuê dịch vụ, đề cương và dự toán chi tiết thuộc thẩm quyền phê duyệt của Tổng cục, đơn vị thuộc Tổng cục.

c) Trường hợp hệ thống thông tin liên quan đến đơn vị thuộc đối tượng áp dụng của Quy chế này nhưng không thuộc phạm vi quy định tại điểm a, b của khoản 1 Điều này, Cục trưởng Cục Tin học và Thống kê tài chính báo cáo Bộ trưởng Bộ Tài chính quyết định đơn vị chủ quản hệ thống thông tin hoặc ủy quyền thực hiện trách nhiệm của chủ quản hệ thống thông tin theo quy định của pháp luật.

2. Đơn vị vận hành hệ thống thông tin:

a) Đơn vị thuộc Cơ quan Bộ (bao gồm Cục Tin học và Thống kê tài chính), đơn vị sự nghiệp trực thuộc Bộ chủ trì xây dựng, thiết lập, nâng cấp, mở rộng, bảo trì, bảo dưỡng, duy trì hoạt động lớp ứng dụng hoặc cơ sở dữ liệu của hệ thống thông tin thực hiện vai trò đơn vị vận hành hệ thống thông tin. Cục Tin học và Thống kê tài chính là đơn vị vận hành hệ thống mạng nội bộ và hệ thống an toàn an ninh mạng của Cơ quan Bộ; hệ thống mạng trục của Hạ tầng truyền thông thống nhất ngành Tài chính và các hệ thống thông tin khác theo quyết định của Bộ trưởng Bộ Tài chính.

b) Đối với hệ thống thông tin do Tổng cục làm chủ quản, Tổng cục chỉ định đơn vị vận hành hệ thống thông tin.

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

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

a) Cục Tin học và Thống kê tài chính đảm nhiệm vai trò đơn vị chuyên trách an toàn an ninh mạng của Bộ Tài chính.

b) Đơn vị chuyên trách công nghệ thông tin trực thuộc Tổng cục đảm nhiệm vai trò đơn vị chuyên trách an toàn an ninh mạng của Tổng cục.

c) Chủ quản hệ thống thông tin thành lập hoặc chỉ định bộ phận chuyên trách an toàn an ninh mạng thuộc đơn vị chuyên trách an toàn an ninh mạng của chủ quản hệ thống thông tin.

4. Ban Chỉ đạo Chuyển đổi số của Bộ Tài chính đồng thời đảm nhiệm vai trò Ban Chỉ đạo ứng cứu sự cố an toàn an ninh mạng Bộ Tài chính.

5. Đơn vị chuyên trách về ứng cứu sự cố an toàn an ninh mạng (gọi tắt là Đơn vị chuyên trách ứng cứu sự cố):

a) Cục Tin học và Thống kê tài chính đảm nhiệm vai trò đơn vị chuyên trách ứng cứu sự cố của Bộ Tài chính, chịu trách nhiệm triển khai công tác ứng cứu sự cố các hệ thống thông tin do Bộ Tài chính làm chủ quản (không bao gồm các hệ thống thông tin mà Bộ đã ủy quyền thực hiện trách nhiệm của chủ quản hệ thống thông tin).

b) Đơn vị chuyên trách an toàn an ninh mạng của Tổng cục đảm nhiệm vai trò đơn vị chuyên trách ứng cứu sự cố của Tổng cục.

c) Đơn vị chuyên trách ứng cứu sự cố trình chủ quản hệ thống thông tin thành lập Đội ứng cứu sự cố và tổ chức hoạt động ứng cứu sự cố trong lĩnh vực, địa bàn, phạm vi mình quản lý.

6. Lực lượng bảo vệ an ninh mạng Bộ Tài chính bao gồm bộ phận chuyên trách an toàn an ninh mạng thuộc Cục Tin học và Thống kê tài chính; bộ phận chuyên trách an toàn an ninh mạng thuộc đơn vị chuyên trách công nghệ thông tin trực thuộc Tổng cục; các Đội ứng cứu sự cố thuộc Bộ Tài chính.

7. Đơn vị, bộ phận được phân công đảm nhiệm vai trò bảo đảm an toàn an ninh mạng tại điểm 1 đến điểm 6 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.

Điều 5. Thẩm quyền thực hiện thủ tục xác định cấp độ an toàn hệ thống thông tin, xác định hệ thống thông tin quan trọng về an ninh quốc gia

1. Thẩm quyền thực hiện thủ tục xác định cấp độ an toàn hệ thống thông tin:

a) Thẩm quyền thực hiện thủ tục xác định cấp độ an toàn hệ thống thông tin thực hiện theo quy định tại Điều 12, 13, 14 Nghị định số 85/2016/NĐ-CP. Đối với hệ thống thông tin đề xuất cấp độ 3 do Bộ Tài chính làm chủ quản (không bao gồm hệ thống thông tin đã được Bộ Tài chính ủy quyền thực hiện trách nhiệm của chủ quản hệ thống thông tin), Bộ trưởng Bộ Tài chính ủy quyền cho Cục trưởng Cục Tin học và Thống kê tài chính ký Quyết định phê duyệt hồ sơ đề xuất cấp độ.

b) Trường hợp đơn vị chuyên trách an toàn an ninh mạng đồng thời là đơn vị vận hành hệ thống thông tin, 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.

2. Thẩm quyền thực hiện thủ tục xác định hệ thống thông tin quan trọng về an ninh quốc gia:

a) Đối với hệ thống thông tin đề xuất cấp độ 4, 5 trong quá trình thẩm định hồ sơ đề xuất cấp độ được cơ quan thẩm định xác định đáp ứng tiêu chí đưa vào

Danh mục hệ thống thông tin quan trọng về an ninh quốc gia, chủ quản hệ thống thông tin báo cáo Lãnh đạo Bộ Tài chính (thông qua Cục Tin học và Thống kê tài chính) và thực hiện điều chỉnh, bổ sung hồ sơ theo hướng dẫn của Bộ Công an (nếu được yêu cầu).

b) Đối với hệ thống thông tin đề xuất cấp độ 1, 2, 3 đáp ứng tiêu chí 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):

- Trường hợp hệ thống thông tin do Bộ Tài chính làm chủ quản, Cục Tin học và Thống kê tài chính phối hợp với đơn vị vận hành hệ thống thông tin lập hồ sơ đề nghị đưa hệ thống vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia, trình Bộ trưởng Bộ Tài chính gửi Bộ Công an thẩm định.

- Trường hợp hệ thống thông tin do Tổng cục làm chủ quản, Tổng cục tổ chức lập hồ sơ đề nghị đưa hệ thống vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia, trình Bộ trưởng Bộ Tài chính (thông qua Cục Tin học và Thống kê tài chính). Sau khi được Lãnh đạo Bộ Tài chính phê duyệt nội dung lấy ý kiến thẩm định, thủ trưởng đơn vị chủ quản hệ thống thông tin thừa lệnh Bộ trưởng, ký công văn gửi Bộ Công an.

Điều 6. Bảo đảm an toàn an ninh mạng đối với hệ thống thông tin, thiết bị xử lý thông tin

1. Chủ quản hệ thống thông tin, đơn vị vận hành hệ thống thông tin, đơn vị chuyên trách an toàn an ninh mạng thực hiện các nhiệm vụ sau:

a) Xác định cấp độ an toàn của hệ thống thông tin (lập hồ sơ đề xuất cấp độ; tổ chức thẩm định, phê duyệt hồ sơ đề xuất cấp độ) và triển khai phương án bảo đảm an toàn hệ thống thông tin theo cấp độ theo quy định từ Điều 13 đến Điều 19 của Nghị định số 85/2016/NĐ-CP; từ Điều 7 đến Điều 10 của Thông tư số 12/2022/TT-BTTTT và khoản 1 Điều 5 của Quy chế này. Việc xác định hệ thống thông tin, bao gồm hệ thống thông tin sử dụng camera giám sát, để xác định cấp độ căn cứ trên nguyên tắc được quy định tại khoản 1 Điều 5 Nghị định 85/2016/NĐ-CP, Điều 7 Thông tư 12/2022/TT-BTTTT và các hướng dẫn bổ sung của Bộ Thông tin và Truyền thông (nếu có).

b) Bảo đảm an ninh mạng cho hệ thống thông tin quan trọng về an ninh quốc gia theo quy định từ Điều 12 đến Điều 15 của Luật An ninh mạng, Điều 7 đến Điều 17 của Nghị định số 53/2022/NĐ-CP.

2. Đơn vị không thuộc phạm vi khoản 1 Điều này và có thẩm quyền tự trang bị thiết bị xử lý thông tin sử dụng tại đơn vị có trách nhiệm:

a) Bảo đảm an toàn an ninh mạng cho máy tính của người sử dụng thuộc đơn vị: sử dụng hệ điều hành được hỗ trợ bản vá lỗ hổng bảo mật; chỉ cài đặt tiện ích thiết yếu được cung cấp kèm theo hệ điều hành và các phần mềm phục vụ công việc, có bản quyền hoặc được các cơ quan chức năng đánh giá, xác nhận an toàn; cài đặt phần mềm phòng, diệt mã độc và cập nhật thường xuyên mẫu nhận diện mã độc.

b) Bảo đảm an toàn an ninh mạng cho thiết bị mạng, thiết bị an ninh mạng sử dụng tại đơn vị: không sử dụng thiết bị không còn được hỗ trợ khắc phục lỗ hổng bảo mật; thực hiện khắc phục lỗ hổng bảo mật ngay khi nhận được cảnh báo, hướng dẫn từ cơ quan chức năng; thay đổi mật khẩu mặc định và giữ bí mật mật khẩu quản trị thiết bị.

3. Đơn vị mua sắm, sử dụng camera giám sát phải tuân thủ quy chuẩn kỹ thuật quốc gia về an toàn thông tin mạng cơ bản cho camera giám sát, theo Chỉ thị số 23/CT-TTg ngày 26/12/2022 của Thủ tướng Chính phủ về tăng cường công tác bảo đảm an toàn thông tin mạng, an ninh thông tin cho thiết bị camera giám sát.

Điều 7. Quản lý rủi ro, lỗ hổng, điểm yếu an toàn an ninh mạng

1. Đơn vị chuyên trách an toàn an ninh mạng phối hợp với đơn vị vận hành hệ thống thông tin tổ chức quản lý lỗ hổng, điểm yếu an toàn an ninh mạng theo các nội dung sau:

a) Lập danh sách toàn bộ thiết bị, phần mềm công nghệ thông tin đang sử dụng trong phạm vi quản lý của chủ quản hệ thống thông tin: nhãn hiệu phần cứng, tên phần mềm và phiên bản (hệ điều hành, cơ sở dữ liệu, ứng dụng, các tiện ích khác).

b) Thiết lập, duy trì kênh tiếp nhận thông tin về lỗ hổng, điểm yếu an toàn an ninh mạng từ các cơ quan, tổ chức có chức năng cảnh báo về an toàn an ninh mạng; các đơn vị cung cấp thiết bị, phần mềm công nghệ thông tin thuộc phạm vi điểm a khoản này.

c) Quản lý, giám sát việc cài đặt bản vá lỗ hổng, điểm yếu an toàn an ninh mạng. Sử dụng và cập nhật liên tục các công cụ dò quét lỗ hổng, điểm yếu an toàn an ninh mạng để các công cụ này có thể phát hiện được các lỗ hổng bảo mật mới nhất; hoặc sử dụng kết quả kiểm tra, đánh giá an toàn an ninh mạng để xác định các lỗ hổng, điểm yếu của hệ thống thông tin.

d) Triển khai cài đặt bản vá lỗ hổng, điểm yếu an toàn an ninh mạng sau khi bản vá được phát hành; Áp dụng các biện pháp bảo vệ tạm thời trong trường hợp bản vá bảo mật chưa được phát hành hoặc chưa đủ điều kiện để triển khai.

2. Đơn vị chuyên trách an toàn an ninh mạng phối hợp với đơn vị vận hành hệ thống thông tin triển khai quản lý rủi ro an toàn an ninh mạng trên cơ sở quản lý lỗ hổng, điểm yếu an toàn an ninh mạng theo quy định tại khoản 1 Điều này và theo hướng dẫn của Bộ Thông tin và Truyền thông, Bộ Công an.

Điều 8. Giám sát an toàn an ninh mạng

1. Đơn vị chuyên trách an toàn an ninh mạng tự thực hiện giám sát hoặc lựa chọn tổ chức, doanh nghiệp có đủ năng lực thực hiện giám sát an toàn hệ thống thông tin theo quy định tại Điều 5 Thông tư số 31/2017/TT-BTTTT và hướng dẫn của Bộ Thông tin và Truyền thông. Cục Tin học và Thống kê tài chính thiết lập hệ thống tiếp nhận thông tin giám sát từ các đơn vị thuộc Bộ Tài chính và

hướng dẫn các đơn vị thuộc Bộ kết nối, chia sẻ thông tin về Bộ Tài chính; làm đầu mối thực hiện kết nối, chia sẻ thông tin giám sát từ các đơn vị của Bộ Tài chính với Trung tâm giám sát không gian mạng quốc gia thuộc Cục An toàn thông tin, Bộ Thông tin và Truyền thông. Nội dung thông tin giám sát cần kết nối, chia sẻ theo hướng dẫn của Bộ Thông tin và Truyền thông.

2. Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia phối hợp với Cục An ninh mạng và phòng chống tội phạm công nghệ cao của Bộ Công an triển khai giám sát an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia theo quy định tại khoản 3 Điều 15 Nghị định số 53/2022/NĐ-CP.

3. Các Tổng cục phối hợp với Cục Tin học và Thống kê tài chính thực hiện chia sẻ thông tin giám sát an toàn hệ thống thông tin với cơ quan chức năng của Bộ Quốc phòng theo hướng dẫn của Bộ Quốc phòng.

Điều 9. Kiểm tra, đánh giá an toàn an ninh mạng

1. Về kiểm tra, đánh giá việc tuân thủ quy định của pháp luật về an toàn an ninh mạng; kiểm tra, đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin theo phương án bảo đảm an toàn thông tin được phê duyệt:

a) Cục Tin học và Thống kê tài chính thực hiện kiểm tra, đánh giá các Tổng cục, các đơn vị thuộc Cơ quan Bộ, đơn vị sự nghiệp trực thuộc Bộ Tài chính trong chương trình, kế hoạch kiểm tra công tác ứng dụng công nghệ thông tin hàng năm hoặc chương trình kiểm tra theo chuyên đề về an toàn an ninh mạng được Bộ trưởng Bộ Tài chính phê duyệt.

b) Các đơn vị thuộc Bộ tự kiểm tra, đánh giá hàng năm trong nội bộ đơn vị, trong phạm vi trách nhiệm của đơn vị đối với công tác an toàn an ninh mạng theo quy định của pháp luật và quy định tại Quy chế này.

2. Chủ quản hệ thống thông tin (hoặc đơn vị chuyên trách an toàn an ninh mạng của chủ quản hệ thống thông tin) lựa chọn tổ chức, doanh nghiệp có chức năng hoặc được cấp phép thực hiện kiểm tra, đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thông tin, theo quy định tại điểm c khoản 2 Điều 20 Nghị định số 85/2016/NĐ-CP và khoản 3 Điều 11, khoản 3 Điều 12 Thông tư số 12/2022/TT-BTTTT; kiểm tra, đánh giá an ninh mạng theo quy định tại điểm c khoản 2 Điều 24 Nghị định số 53/2022/NĐ-CP và theo hướng dẫn của Bộ Công an. Tổ chức, doanh nghiệp cung cấp dịch vụ kiểm tra, đánh giá an toàn an ninh mạng phải độc lập với tổ chức, doanh nghiệp cung cấp dịch vụ giám sát an toàn, an ninh mạng cho đơn vị.

Điều 10. Ứng phó sự cố an toàn an ninh mạng

1. Cục Tin học và Thống kê tài chính, Tổng cục xây dựng, 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 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-BTTT (đối

với hệ thống cấp độ 1, 2, 3) và quy định tại Điều 25 của Nghị định số 53/2022/NĐ-CP; tổ chức triển khai kế hoạch, phương án sau khi phê duyệt. Đối với nội dung (thuộc kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng; phương án ứng phó, khắc phục sự cố an ninh mạng) vượt thẩm quyền quyết định của đơn vị, đơn vị lấy ý kiến của các đơn vị liên quan, báo cáo Lãnh đạo Bộ Tài chính xem xét, quyết định.

2. Đối với hệ thống thông tin không phải hệ thống thông tin quan trọng về an ninh quốc gia, áp dụng quy trình ứng cứu sự cố thông thường theo quy định tại Điều 11 Thông tư 20/2017/TT-BTTTT; áp dụng quy trình ứng cứu sự cố nghiêm trọng theo quy định tại Điều 14 Quyết định 05/2017/QĐ-TTg. Đối với hệ thống thông tin quan trọng về an ninh quốc gia, áp dụng trình tự, thủ tục ứng phó, khắc phục sự cố an ninh mạng theo quy định tại Điều 17 của Nghị định số 53/2022/NĐ-CP. Trong quá trình ứng cứu, ứng phó sự cố đối với hệ thống thông tin cấp độ 4, 5 và hệ thống thông tin quan trọng về an ninh quốc gia, các Tổng cục có trách nhiệm báo cáo Lãnh đạo Bộ Tài chính, đồng thời cung cấp thông tin diễn biến tình hình cho Cục Tin học và Thống kê tài chính để phối hợp xử lý.

3. Đơn vị chuyên trách an toàn an ninh mạng có trách nhiệm theo dõi, nắm bắt thông tin trên phương tiện thông tin đại chúng và mạng Internet về các sự kiện mất an toàn an ninh mạng có thể tác động tới đơn vị; chủ động 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 (gửi trực tiếp cho đơn vị hoặc do Văn phòng Bộ, Cục Tin học và Thống kê tài chính sao gửi chủ quản hệ thống thông tin); Thiết lập kênh trao đổi thông tin với các đối tác cung cấp thiết bị, phần mềm, giải pháp an toàn thông tin của đơn vị để nắm bắt kịp thời vấn đề, sự cố có khả năng tác động tới hệ thống thông tin của đơn vị. Đơn vị chuyên trách an toàn an ninh mạng cử 01 lãnh đạo chịu trách nhiệm triển khai công tác an toàn an ninh mạng và 01 cán bộ làm đầu mối tiếp nhận cảnh báo an toàn thông tin từ Cục Tin học và Thống kê tài chính, các cơ quan, tổ chức có chức năng cảnh báo an toàn thông tin mạng, an ninh mạng (thông qua thư điện tử hoặc các kênh trao đổi thông tin khác).

4. Khi xảy ra sự cố an toàn thông tin mạng thuộc loại hình tấn công mạng, đơn vị vận hành hệ thống thông tin thực hiện báo cáo theo quy định tại Điều 11 Quyết định 05/2017/QĐ-TTg và Điều 9 Thông tư 20/2017/TT-BTTTT, đồng thời gửi báo cáo cho Cục Tin học và Thống kê tài chính để tổng hợp, báo cáo Lãnh đạo Bộ Tài chính. Chủ quản hệ thống thông tin phải thông báo rộng rãi về đầu mối tiếp nhận thông tin để các cá nhân, tổ chức thuộc đơn vị liên lạc trong trường hợp: nghi ngờ, phát hiện dấu hiệu tấn công, sự cố an toàn thông tin mạng; dấu hiệu, hành vi khủng bố mạng; tình huống nguy hiểm về an ninh mạng; hành vi vi phạm pháp luật về an ninh mạng liên quan đến các hệ thống thông tin do đơn vị quản lý.

5. Định kỳ hàng năm, Cục Tin học và Thống kê tài chính chủ trì tổ chức diễn tập thực chiến an toàn an ninh mạng cho các đơn vị thuộc Bộ Tài chính, theo kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng và phương án ứng

phó, khắc phục sự cố an ninh mạng được phê duyệt, trong phạm vi các hệ thống thông tin do Bộ Tài chính làm chủ quản. Các Tổng cục tổ chức huấn luyện, diễn tập ứng cứu sự cố theo kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng và phương án ứng phó, khắc phục sự cố an ninh mạng được phê duyệt, trong phạm vi các hệ thống thông tin do đơn vị làm chủ quản. Đơn vị là thành viên mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia tham gia đầy đủ các cuộc diễn tập quốc gia, quốc tế do Cơ quan điều phối quốc gia và các cơ quan chức năng thuộc Bộ Thông tin và Truyền thông, Bộ Công an, Bộ Quốc phòng tổ chức.

6. Cục Tin học và Thống kê tài chính; đơn vị chuyên trách an toàn an ninh mạng thuộc Tổng cục Thuế, Tổng cục Hải quan, Kho bạc Nhà nước có trách nhiệm đăng ký tham gia Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia. Khuyến khích các đơn vị khác thuộc Bộ phù hợp tiêu chí quy định tại khoản 2 Điều 7 Quyết định số 05/2017/QĐ-TTg đăng ký tham gia Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia với tư cách thành viên tự nguyện.

Điều 11. Phòng ngừa, xử lý hành vi xâm phạm an ninh mạng

1. Đơn vị chuyên trách an toàn an ninh mạng của chủ quản hệ thống thông tin phối hợp với đơn vị vận hành hệ thống thông tin thực hiện các nhiệm vụ sau trong phạm vi hệ thống thông tin thuộc quản lý của chủ quản hệ thống thông tin, 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 có nội dung: tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; làm nhục, vu khống; xâm phạm trật tự quản lý kinh tế trên hệ thống thông tin;

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, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời tư trên hệ thống thông tin và kịp thời gỡ bỏ thông tin liên quan đến hành vi này;

c) Áp dụng 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, thực hiện yêu cầu của Cục An ninh mạng và Phòng, chống tội phạm sử dụng công nghệ cao (Bộ Công an) về phòng, chống gián điệp mạng, bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời tư trên hệ thống thông tin; về áp dụng biện pháp 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; về gỡ bỏ các nội dung buộc phải

gỡ bỏ theo quy định của pháp luật trên hệ thống thông tin; về thực hiện biện pháp phòng ngừa, phát hiện, xử lý tình huống nguy hiểm về an ninh mạng.

2. Đơn vị chuyên trách an toàn an ninh mạng của chủ quản hệ thống thông tin khi tiếp nhận tin báo về tình huống nguy hiểm 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.

3. Chủ quản hệ thống thông tin có trách nhiệm thông báo cho Cục An ninh mạng và Phòng, chống tội phạm sử dụng công nghệ cao khi phát hiện hành vi vi phạm pháp luật về an ninh mạng trên hệ thống thông tin thuộc phạm vi quản lý.

Điều 12. Phổ biến, tuyên truyền, đào tạo, bồi dưỡng về an toàn an ninh mạng

1. Cục Tin học và Thống kê tài chính phối hợp với Văn phòng Bộ và các đơn vị liên quan lập kế hoạch và triển khai công tác tuyên truyền, phổ biến chủ trương, chính sách, pháp luật, biện pháp an toàn an ninh mạng, thông qua các hình thức: văn bản hướng dẫn; hội nghị, hội thảo; đăng bài trên Cổng thông tin điện tử Bộ Tài chính, báo, tạp chí của ngành Tài chính; gửi thư điện tử và các hình thức khác phù hợp với quy định của pháp luật. Các đơn vị thuộc Bộ Tài chính có trách nhiệm thực hiện quán triệt, tuyên truyền, phổ biến, nâng cao nhận thức, trách nhiệm về an toàn an ninh mạng cho cán bộ, công chức, viên chức, người lao động thuộc đơn vị.

2. Cục Tin học và Thống kê tài chính tổ chức đào tạo, bồi dưỡng theo các chương trình đào tạo ngắn hạn nâng cao kiến thức, kỹ năng về an toàn an ninh mạng cho công chức, viên chức chuyên trách về công nghệ thông tin, an toàn an ninh mạng tại các đơn vị thuộc Bộ Tài chính. Trường Bồi dưỡng cán bộ Bộ Tài chính phối hợp với Cục Tin học và Thống kê tài chính tổ chức bồi dưỡng kiến thức cơ bản, kỹ năng về an toàn an ninh mạng cho cán bộ quản lý, nghiệp vụ các đơn vị thuộc Bộ Tài chính. Tổng cục, đơn vị sự nghiệp trực thuộc Bộ tổ chức đào tạo, bồi dưỡng hoặc cử cán bộ của đơn vị tham gia đào tạo, bồi dưỡng về an toàn an ninh mạng.

Điều 13. Báo cáo an toàn an ninh mạng

1. Đối với báo cáo năm về an toàn thông tin mạng, chủ quản hệ thống thông tin lập báo cáo theo quy định tại khoản 3 Điều 13 và Điều 14 Thông tư số 12/2022/TT-BTTTT gửi Cục Tin học và Thống kê tài chính trước ngày 20 tháng 12 hàng năm. Cục Tin học và Thống kê tài chính tổng hợp, xây dựng Báo cáo an toàn thông tin định kỳ hàng năm của Bộ Tài chính, trình Lãnh đạo Bộ phê duyệt, gửi Bộ Thông tin và Truyền thông trước ngày 25 tháng 12 hàng năm.

2. Cục Tin học và Thống kê tài chính lập Báo cáo hoạt động giám sát an toàn thông tin mạng của Bộ Tài chính định kỳ 6 tháng theo quy định tại điểm k

khoản 3 Điều 5 Thông tư số 31/2017/TT-BTTTT, trình Lãnh đạo Bộ phê duyệt, gửi Bộ Thông tin và Truyền thông.

3. Thành viên mạng lưới ứng cứu sự cố an toàn không gian mạng quốc gia 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, đồng thời gửi Cục Tin học và Thống kê tài chính để theo dõi; và thực hiện các báo cáo khác theo quy định tại Thông tư số 20/2017/TT-BTTTT.

4. Cục Tin học và Thống kê tài chính chủ trì, phối hợp với các chủ quản hệ thống thông tin thuộc Bộ Tài chính xây dựng các báo cáo đột xuất về an toàn an ninh mạng theo yêu cầu của Bộ Thông tin và Truyền thông, Bộ Công an, Bộ Quốc phòng, trình Lãnh đạo Bộ Tài chính phê duyệt.

Chương III
QUY ĐỊNH VỀ AN TOÀN AN NINH MẠNG TẠI CƠ QUAN BỘ

Điều 14. Quy định về tài khoản thông tin

1. Tài khoản thông tin (gọi tắt là tài khoản) là tập hợp gồm tên đăng nhập và mật khẩu hoặc/và 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 tại Bộ Tài chính; bao gồm các loại sau:

a) Tài khoản định danh: mỗi tài khoản định danh chỉ 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.

b) Tài khoản truy cập hệ thống gắn với một nhiệm vụ cụ thể, được gắn với quyền truy cập thực hiện các tác vụ cần thiết cho nhiệm vụ đó (ví dụ: tài khoản văn thư, tài khoản biên tập,...).

c) 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.

2. Cục Tin học và Thống kê tài chính cấp tài khoản định danh cho người dùng tại Cơ quan Bộ trong thời gian không quá 03 ngày làm việc, tính từ thời điểm nhận được văn bản đề nghị cấp tài khoản của đơn vị quản lý người dùng; điều chỉnh quyền truy cập, thu hồi tài khoản định danh của cá nhân thay đổi vị trí việc làm hoặc dừng làm việc tại Cơ quan Bộ trong thời gian không quá 03 ngày làm việc tính từ ngày người dùng chính thức được bổ nhiệm, điều động, chuyển công tác, thôi việc, nghỉ hưu hoặc từ thời điểm nhận được văn bản đề nghị dừng tài khoản của đơn vị quản lý người dùng. Trường hợp cần duy trì tài khoản định danh sau thời điểm người dùng dừng làm việc tại Cơ quan Bộ, đơn vị quản lý người dùng phải có văn bản gửi Cục Tin học và Thống kê tài chính, trong đó nêu rõ lý do, phạm vi các quyền cần duy trì và thời gian duy trì tài khoản.

3. Cục Tin học và Thống kê tài chính hoặc đơn vị vận hành hệ thống thông tin cấp tài khoản nhiệm vụ cho người dùng được đơn vị quản lý người dùng phân công thực hiện nhiệm vụ. 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 giao trả tài khoản cho đơn vị quản lý người dùng.

4. 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. Cục Tin học và Thống kê tài chính giữ ít nhất 01 tài khoản quản trị hệ điều hành của tất cả các máy chủ hoạt động trong mạng nội bộ Cơ quan Bộ. 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.

5. 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 khác trên bàn phím máy tính (` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? /) và dấu cách; không chứa tên tài khoản. Khuyến khích sử dụng mật khẩu có độ dài từ 12 ký tự trở lên.

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.

6. Cá nhân được cấp hoặc giao 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 an ninh mạng.

7. Cục Tin học và Thống kê tài chính, đơn vị vận hành hệ thống thông tin thường xuyên rà soát các tài khoản đang hoạt động, phát hiện và thu hồi các tài khoản không sử dụng hoặc không hợp lệ, điều chỉnh thông tin tài khoản chưa phản ánh chính xác thông tin thực tế tại thời điểm rà soát.

Điều 15. Quy định về máy tính của người dùng

1. Máy tính do các đơn vị thuộc Cơ quan Bộ trang bị có kết nối vào mạng nội bộ phải đáp ứng đầy đủ các yêu cầu sau:

a) Đặt tên máy theo quy tắc:

- Đối với máy cá nhân: Tên viết tắt của đơn vị (theo quy định của Bộ Tài chính)-Số phòng-Tên của người dùng *(ví dụ: THTK-212-AN)*, trường hợp trong một phòng có người trùng tên thì thêm Họ và tên đệm (ví dụ: *THTK-212-ANNT*) và thêm số thứ tự (nếu cần thiết);

- Đối với máy dùng chung: hoặc Tên viết tắt của đơn vị-Số phòng-Chức năng dùng chung (*ví dụ: THTK-210-ANNINH).*

b) Sử dụng hệ điều hành được hỗ trợ bản vá lỗ hổng bảo mật; trường hợp đã hết hỗ trợ phải có kế hoạch nâng cấp, thay thế. Chỉ cài đặt tiện ích thiết yếu được cung cấp kèm theo hệ điều hành và các phần mềm phục vụ công việc, có bản quyền hoặc được các cơ quan chức năng đánh giá, xác nhận an toàn. Cài đặt phần mềm phòng diệt mã độc và cập nhật mẫu nhận diện mã độc từ hệ thống quản lý phần mềm phòng diệt mã độc tập trung do Cục Tin học và Thống kê tài chính vận hành.

c) Không kết nối với mạng không dây (wifi), mạng dữ liệu di động (3G/4G/5G...).

d) Căn cứ yêu cầu về bảo đảm an toàn an ninh mạng, Cục Tin học và Thống kê tài chính có thể cài đặt thêm phần mềm giám sát an toàn an ninh mạng đối với các máy tính đáp ứng hiệu năng yêu cầu.

đ) Máy tính trước khi kết nối vào mạng nội bộ Bộ Tài chính phải được Cục Tin học và Thống kê tài chính kiểm tra đáp ứng các quy định tại điểm a, b, c của khoản này. Cục Tin học và Thống kê tài chính có trách nhiệm giám sát, đảm bảo máy tính kết nối vào mạng nội bộ tuân thủ các quy định tại khoản này; ngắt kết nối mạng của máy tính không đáp ứng quy định.

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

2. Máy tính soạn thảo văn bản chứa nội dung bí mật nhà nước, lưu trữ 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, mạng nội bộ, mạng không dây, mạng viễn thông, trừ trường hợp đã áp dụng các biện pháp bảo vệ theo hướng dẫn của Ban Cơ yếu Chính phủ. Không sử dụng thiết bị lưu trữ ngoài không do Ban Cơ yếu Chính phủ cung cấp, trừ trường hợp cần cài đặt hệ điều hành, sửa chữa, nâng cấp phần mềm cho máy tính hoặc phục vụ công tác kiểm tra, thanh tra về an toàn an ninh mạng.

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

c) Trường hợp ổ cứng lỗi cần mang đi bảo hành, phải thực hiện biện pháp xóa dữ liệu vĩnh viễn 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, phải 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 trong quá trình này (có biên bản giữa đơn vị sử dụng máy tính và đơn vị sửa chữa, nâng cấp phần mềm).

d) Đơn vị được cấp sử dụng máy tính soạn thảo, lưu trữ bí mật nhà nước chịu trách nhiệm giám sát, đảm bảo việc sử dụng máy tính tuân thủ đúng quy định tại khoản này.

3. Trường hợp máy tính xách tay được cơ quan trang bị để sử dụng bên ngoài trụ sở Bộ, nếu kết nối Internet, phải cài đặt hệ điều hành được hỗ trợ bản vá lỗ hổng bảo mật và phần mềm phòng diệt mã độc, phải cập nhật thường xuyên bản vá cho hệ điều hành và mẫu nhận diện mã độc do nhà sản xuất cung cấp.

4. Đối với máy tính bảng được cơ quan trang bị để phục vụ công việc phải sử dụng hệ điều hành được hỗ trợ bản vá lỗ hổng bảo mật; chỉ cài đặt phần mềm phục vụ công việc và các phần mềm bảo đảm an toàn an ninh mạng do Cục Tin học và Thống kê tài chính hoặc các cơ quan chức năng về an toàn an ninh mạng cung cấp; cấu hình bảo đảm an toàn an ninh mạng theo hướng dẫn của Cục Tin học và Thống kê tài chính.

5. Máy tính do người dùng tự trang bị, khi kết nối vào mạng nội bộ hoặc chạy ứng dụng của Bộ Tài chính từ địa điểm bên ngoài mạng nội bộ của Bộ Tài chính, phải đáp ứng đầy đủ các điều kiện dưới đây:

a) Cài đặt đầy đủ các bản vá lỗ hổng bảo mật của hệ điều hành; cài đặt phần mềm phòng diệt mã độc và cập nhật mẫu nhận diện mã độc mới nhất;

b) Không cài đặt, sử dụng phần mềm, công cụ có tính năng hoặc tạo rủi ro mất an toàn an ninh mạng (cấp phát địa chỉ mạng, dò quét mật khẩu, dò quét cổng mạng, giả lập tấn công...);

c) Khi kết nối vào mạng nội bộ Bộ Tài chính, người dùng cần thực hiện: ngắt các kết nối vào các hệ thống mạng khác (mạng không dây, mạng dữ liệu di động...), không sử dụng máy tính như một điểm phát sóng không dây.

Điều 16. Quy định đối với người dùng

Người dùng tại cơ quan Bộ Tài chính có trách nhiệm:

1. Đảm bảo an toàn mật khẩu các tài khoản thông tin mà người dùng được cấp, theo quy định tại khoản 5 Điều 14 của Quy chế này. Nếu phát hiện có dấu hiệu lộ mật khẩu, thực hiện các việc sau: đổi mật khẩu tại máy tính làm việc tại cơ quan; quét mã độc trên các thiết bị của cá nhân đã từng được sử dụng để truy cập thư điện tử công vụ hoặc các ứng dụng của Bộ Tài chính trước đó; cung cấp thông tin về sự việc, hiện tượng cho bộ phận hỗ trợ kỹ thuật của Cục Tin học và Thống kê tài chính.

2. Sử dụng tài khoản định danh cá nhân khi đăng nhập vào máy tính có kết nối vào mạng nội bộ.

3. Truy cập sử dụng Internet từ máy tính có kết nối mạng nội bộ phải thông qua hệ thống Internet an toàn do Cục Tin học và Thống kê tài chính thiết lập.

4. 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 (F:

cá nhân người dùng, P: phòng/đơn vị cấp tương đương, Q: Vụ/Cục/Đơn vị cấp tương đương, T: toàn bộ người dùng tại trụ sở Bộ). Xóa thông tin trên ổ đĩa mạng do bản thân tạo ra sau khi thông tin hết giá trị sử dụng.

5. Nếu nghi ngờ hoặc phát hiện thư điện tử nhận được là thư rác, thư giả mạo, người dùng chuyển tiếp thư này cho bộ phận hỗ trợ kỹ thuật của Cục Tin học và Thống kê tài chính để áp dụng biện pháp ngăn chặn. 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 mở thư điện tử công vụ và các phần mềm nội bộ của Bộ Tài chính trên máy tính công cộng hoặc máy tính không đáp ứng các yêu cầu quy định tại khoản 3, 4, 5 Điều 15 của Quy chế này. Không sử dụng địa chỉ thư điện tử công vụ để đăng ký sử dụng các ứng dụng, dịch vụ ngoài phạm vi công việc. Mã hóa (đặt mật khẩu) các tệp tin có nội dung nhạy cảm trước khi gửi qua thư điện tử và gửi mật khẩu cho người nhận bằng phương thức khác.

6. Thực hiện quét mã độc thiết bị lưu trữ ngoài (thẻ nhớ, ổ đĩa ngoài,...) trước khi sử dụng. Bảo vệ thiết bị lưu trữ ngoài, không để thất thoát thông tin, tài liệu của cơ quan. Mã hóa (đặt mật khẩu) các tệp tin có nội dung nhạy cảm khi lưu trữ trên thiết bị lưu trữ ngoài và xóa thông tin, tài liệu của cơ quan trên thiết bị lưu trữ ngoài sau khi hoàn thành xử lý công việc cần sử dụng thiết bị lưu trữ ngoài.

7. Thực hiện soạn thảo văn bản chứa nội dung bí mật nhà nước, lưu trữ tài liệu mật tại máy tính được trang bị cho việc soạn thảo, lưu trữ văn bản mật theo quy định. Không sử dụng thiết bị lưu trữ ngoài để lưu thông tin, tài liệu mật, trừ trường hợp có áp dụng các biện pháp mã hóa do Ban Cơ yếu Chính phủ cung cấp.

8. Đối với bí mật công tác, bí mật kinh doanh, dữ liệu cá nhân do người dùng được phân công xử lý: áp dụng mã hóa dữ liệu trong trường hợp cần lưu trữ, truyền đưa trên môi trường mạng hoặc thiết bị lưu trữ ngoài; giới hạn phạm vi truy cập trong phạm vi các cá nhân có trách nhiệm tham gia xử lý.

9. Khoá máy tính (sử dụng tính năng của hệ điều hành) khi rời khỏi nơi đặt máy tính; tắt máy tính khi rời khỏi cơ quan.

10. Cập nhật bản vá hệ điều hành và quét mã độc thường xuyên máy tính xách tay hoặc máy do người dùng tự trang bị và sử dụng để truy cập ứng dụng của Bộ Tài chính từ Internet.

11. Phối hợp với Cục Tin học và Thống kê tài chính trong việc triển khai các biện pháp an toàn an ninh 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), điều tra nguyên nhân mất an toàn an ninh mạng liên quan đến người dùng hoặc máy tính của người dùng.

Điều 17. Quy định về hệ thống mạng nội bộ

1. Hệ thống mạng nội bộ Cơ quan Bộ Tài chính phải được tổ chức thành các vùng mạng theo chức năng, tối thiểu gồm: vùng mạng người dùng; vùng mạng kết nối Internet; vùng mạng kết nối với các đơn vị trong ngành Tài chính; vùng mạng kết nối với cơ quan, đơn vị ngoài ngành Tài chính và mạng truyền số liệu chuyên dùng Chính phủ; vùng mạng máy chủ cung cấp ứng dụng, dịch vụ ra Internet; vùng mạng máy chủ nội bộ, máy chủ cơ sở dữ liệu; vùng mạng hệ thống quản lý tập trung, quản trị thiết bị; vùng mạng phục vụ công tác quản trị; vùng mạng hệ thống giám sát an toàn an ninh mạng. Sử dụng tường lửa mạng để kiểm soát truy cập giữa các vùng mạng: Chỉ cho phép truy cập các ứng dụng, dịch vụ theo từng ứng dụng, dịch vụ cụ thể; chặn tất cả truy cập tới các dịch vụ, ứng dụng không sử dụng hoặc không phục vụ công việc. Thiết lập phòng chống xâm nhập và phòng chống phần mềm độc hại trên môi trường mạng cho các vùng mạng máy chủ.

2. Các kết nối mạng để xác thực, truy cập thông tin, trao đổi thông tin, quản trị ứng dụng/thiết bị/hệ thống phải áp dụng mã hóa.

3. Các thiết bị mạng lõi, thiết bị mạng các vùng mạng máy chủ, thiết bị an toàn an ninh mạng phải được cấu hình gửi nhật ký hệ thống tới hệ thống giám sát an toàn an ninh mạng. Nhật ký hệ thống của các thiết bị mạng phải được lưu trữ tối thiểu 03 tháng.

4. Các thiết bị mạng phải được cấu hình xác thực để xác thực truy cập quản trị. Chỉ cho phép truy cập quản trị thiết bị mạng từ vùng mạng phục vụ công tác quản trị.

5. Truy cập quản trị hệ thống từ Internet phải thông qua cổng truy cập SSL VPN của Bộ Tài chính và thực hiện xác thực 02 yếu tố; Thiết lập giới hạn thời gian chờ để đóng phiên kết nối khi cổng SSL VPN không nhận được tín hiệu từ người truy cập (tối đa 60 phút).

6. Các thiết bị kết nối vào mạng nội bộ phải đồng bộ thời gian với máy chủ thời gian (được đồng bộ với nguồn thời gian tin cậy trên Internet).

7. Thiết bị mạng, thiết bị an toàn an ninh mạng phải được xử lý lỗ hổng, điểm yếu đã công bố trước khi đưa vào sử dụng và khi có cảnh báo về lỗ hổng bảo mật mới. Thực hiện kiểm tra, đánh giá an toàn an ninh mạng đối với hệ thống mạng nội bộ định kỳ hàng năm.

8. Mạng không dây chỉ phục vụ kết nối Internet cho thiết bị di động. Không thiết lập kết nối vật lý giữa mạng nội bộ với mạng không dây.

9. Tài liệu mô tả hệ thống mạng phải được cập nhật thường xuyên, phản ánh chính xác thực tế các cấu hình, chính sách đang áp dụng cho hệ thống mạng.

Điều 18. Quy định về kết nối Internet

1. Tất cả các kết nối Internet từ mạng nội bộ phải thông qua hệ thống bảo vệ truy cập Internet (có tính năng lọc bỏ, không cho phép truy nhập các trang tin

có nghi ngờ chứa mã độc hoặc các nội dung không phù hợp). Trường hợp việc sử dụng ứng dụng, dịch vụ trên Internet có tính năng đặc biệt không được hỗ trợ bởi hệ thống bảo vệ truy cập Internet, việc truy cập Internet phải thông qua tường lửa mạng.

2. Từ máy trạm có kết nối mạng nội bộ, người sử dụng truy cập Internet thông qua hệ thống Internet an toàn (gồm các máy chủ trung gian ngăn cách máy trạm của người dùng và mạng Internet). Trường hợp người dùng cần sử dụng ứng dụng, dịch vụ mà hệ thống Internet an toàn không hỗ trợ, đơn vị quản lý người dùng gửi yêu cầu hỗ trợ tới Cục Tin học và Thống kê tài chính để được hỗ trợ.

3. Đối với máy chủ và thiết bị xử lý thông tin khác, chỉ thiết lập kết nối Internet cho các hệ thống được thiết kế có giao tiếp với Internet.

Điều 19. Quy định về hệ thống thông tin

1. Phần mềm ứng dụng triển khai trên hệ thống mạng nội bộ của Bộ Tài chính phải đáp ứng các yêu cầu sau:

a) Áp dụng Khung phát triển phần mềm an toàn theo hướng dẫn của Bộ Thông tin và Truyền thông.

b) Sử dụng hệ điều hành, 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 hoạt động trên hệ thống mạng.

c) Có kiến trúc phù hợp với phân chia vùng mạng quy định tại khoản 1 Điều 17 của Quy chế này. Truy cập ứng dụng web phải thông qua tường lửa ứng dụng web; sử dụng chứng thư số SSL đặt trên tường lửa ứng dụng web để mã hóa kết nối giữa người dùng, người quản trị và hệ thống thông tin. Tách riêng địa chỉ truy cập dành cho người dùng và truy cập dành cho quản trị ứng dụng; địa chỉ quản trị ứng dụng không được phép truy cập trực tiếp từ Internet.

d) Có khả năng tích hợp với hệ thống quản lý người dùng tập trung để xác thực người dùng tại cơ quan Bộ. Có tính năng cho phép người dùng đổi mật khẩu. Cho phép cấu hình đảm bảo an toàn mật khẩu người sử dụng đối với tài khoản xác thực tại ứng dụng: Yêu cầu thay đổi mật khẩu mặc định; Cho phép thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự; Cho phép thiết lập thời gian yêu cầu thay đổi mật khẩu; Cho phép thiết lập thời gian mật khẩu hợp lệ; Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định. Mã hóa thông tin xác thực đối với tài khoản xác thực tại ứng dụng theo tiêu chuẩn mã hóa do Bộ Thông tin và Truyền thông quy định. Cho phép cấu hình giới hạn thời gian chờ để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng (cấu hình ban đầu 60 phút và điều chỉnh trong quá trình hoạt động để phù hợp với yêu cầu thực tế của từng ứng dụng).

đ) Có tính năng kiểm tra tính hợp lệ của dữ liệu đầu vào, đầu ra; lọc bỏ, ngăn chặn dữ liệu không hợp lệ.

e) Có tính năng ghi nhật ký hệ thống và gửi nhật ký hệ thống tới hệ thống giám sát an toàn an ninh mạng. Giới hạn kích thước tệp nhật ký hệ thống lưu trên máy chủ ở mức độ phù hợp để không làm ảnh hưởng đến hiệu năng của ứng dụng. Nhật ký hệ thống của ứng dụng phải được lưu trữ tối thiểu 03 tháng.

g) Có phương án sao lưu dự phòng sự cố sử dụng hệ thống sao lưu dữ liệu do Cục Tin học và Thống kê tài chính quản lý.

h) Có thiết kế đáp ứng yêu cầu bảo đảm an toàn hệ thống thông tin theo cấp độ. Khi có thay đổi thiết kế, phải đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống.

i) Áp dụng biện pháp bảo vệ theo hướng dẫn của Ban Cơ yếu Chính phủ đối với ứng dụng có xử lý bí mật nhà nước.

2. Dữ liệu xử lý trong hệ thống thông tin:

a) Trường hợp hệ thống thông tin cần thu thập, xử lý, lưu trữ dữ liệu cá nhân, phải đáp ứng các yêu cầu sau: Chỉ thu thập các dữ liệu cá nhân được phép thu thập theo quy định của pháp luật; Thông báo tới người dùng các loại dữ liệu cá nhân được thu thập, xử lý, lưu trữ thông tin trong hệ thống thông tin và biện pháp bảo vệ; Chỉ cơ quan, đơn vị có trách nhiệm được phân quyền truy cập, sử dụng dữ liệu cá nhân.

b) Bí mật nhà nước của ngành Tài chính phải được mã hoá bằng giải pháp do Ban Cơ yếu Chính phủ cung cấp.

c) Áp dụng chữ ký số trong trường hợp cần đảm bảo chống từ chối nguồn gốc dữ liệu.

3. Máy chủ hoạt động trên hệ thống mạng nội bộ Bộ Tài chính phải đáp ứng các yêu cầu sau:

a) Đặt tên máy theo quy tắc: Viết tắt tên của hệ thống thông tin-Viết tắt chức năng của máy chủ và số thứ tự (nếu có từ 2 máy trở lên cùng chức năng) *(ví dụ: VBDH-APP01)*.

b) Sử dụng hệ điều hành được cung cấp bản vá lỗ hổng, điểm yếu. Chỉ cài đặt các dịch vụ, tiện ích thiết yếu được cung cấp kèm theo hệ điều hành và các phần mềm phục vụ hoạt động của máy chủ, có nguồn gốc an toàn và không nhiễm mã độc. Cài đặt phần mềm phòng diệt mã độc và cập nhật mẫu nhận diện mã độc từ hệ thống quản lý phần mềm phòng diệt mã độc tập trung do Cục Tin học và Thống kê tài chính vận hành; Cài đặt phần mềm giám sát an toàn an ninh mạng. Cấu hình tự động tải bản vá lỗ hổng bảo mật mức hệ điều hành từ hệ thống quản lý bản vá lỗ hổng bảo mật tập trung (đối với máy chủ sử dụng hệ điều hành Windows).

c) Thiết lập chính sách xác thực trên máy chủ đáp ứng quy định về mật khẩu của tài khoản thông tin quy định tại khoản 5 Điều 14 của Quy chế này; yêu cầu thay đổi mật khẩu mặc định. Cấu hình giới hạn thời gian chờ để đóng phiên kết nối khi máy chủ không nhận được yêu cầu từ người dùng (tối đa 60 phút).

d) Cấu hình gửi nhật ký hệ thống tới hệ thống giám sát an toàn an ninh mạng. Nhật ký hệ thống của máy chủ phải được lưu trữ tối thiểu 03 tháng.

đ) Không kết nối với mạng không dây, mạng dữ liệu di động.

e) Thực hiện cài đặt bản vá lỗ hổng bảo mật mức hệ điều hành trong vòng 07 ngày làm việc sau khi bản vá được phát hành.

g) Không lưu mã nguồn ứng dụng; tài liệu thiết kế, cài đặt, quản trị, vận hành, bảo đảm an toàn an ninh mạng hệ thống thông tin trên máy chủ không có chức năng lưu trữ mã nguồn và tài liệu về hệ thống thông tin.

4. Hệ thống thông tin phải được triển khai, cấu hình và duy trì hoạt động đáp ứng các quy định tại Điều này và theo phương án bảo đảm an toàn thông tin đã được phê duyệt theo hồ sơ đề xuất cấp độ; được kiểm tra, đánh giá an toàn an ninh mạng trước khi đưa vào sử dụng và định kỳ hàng năm trong quá trình vận hành.

5. Tài liệu về hệ thống thông tin phải được cập nhật trong quá trình vận hành, đảm bảo phản ánh chính xác hiện trạng của hệ thống. 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.

Điều 20. Quy định về 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; hoặc sử dụng phiên bản phần mềm có lỗ hổng bảo mật nghiêm trọng và không có biện pháp ngăn chặn việc khai thác các lỗ hổng bảo mật này; hoặc các thành phần tài sản của hệ thống thông tin 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.

2. 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) Cục Tin học và Thống kê tài chính thực hiện sao lưu dữ liệu hệ thống thông tin; dừng hoạt động của hệ thống; thu hồi tài nguyên máy chủ ảo hóa (nếu hệ thống thông tin sử dụng nền tảng ảo hóa) hoặc xóa bỏ hoàn toàn (không có khả năng phục hồi) nội dung thông tin, dữ liệu trên thiết bị vật lý trước khi chuyển sang bộ phận quản lý tài sản chờ thanh lý; thu hồi địa chỉ mạng, cấu hình trên hệ thống mạng, hệ thống an toàn an ninh mạng áp dụng cho hệ thống thông tin.

Điều 21. Quy định về sao lưu dữ liệu phòng ngừa sự cố

1. Cục Tin học và Thống kê tài chính thực hiện sao lưu thông tin, dữ liệu của hệ thống thông tin thuộc phạm vi quản lý của Cục và các đơn vị thuộc Cơ quan Bộ như sau:

a) Loại dữ liệu cần sao lưu: Cơ sở dữ liệu, thông tin về cấu hình của phần mềm nội bộ, thông tin cấu hình thiết bị, hệ điều hành của thiết bị và những thông tin, dữ liệu khác (nếu có) thuộc môi trường sản xuất, môi trường dự phòng cần phải sao lưu phục vụ công tác quản lý, khai thác sử dụng.

b) Đối với cơ sở dữ liệu, thông tin về cấu hình của phần mềm nội bộ: Thực hiện sao lưu ngoài giờ hành chính.

c) Đối với thông tin cấu hình thiết bị, hệ điều hành của thiết bị và những thông tin, dữ liệu khác (nếu có): Thực hiện sao lưu 01 bản sao lưu sau mỗi lần cài đặt, thay đổi cấu hình.

d) Lưu giữ tối thiểu 07 bản sao lưu gần nhất.

2. Dữ liệu sao lưu được khôi phục trong các trường hợp: có yêu cầu khôi phục dữ liệu từ người dùng; ứng dụng, cơ sở dữ liệu đang hoạt động bị sự cố, cần khôi phục từ bản sao lưu; hoặc theo yêu cầu của cơ quan có thẩm quyền.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 22. Trách nhiệm của các cơ quan, đơn vị thuộc Bộ Tài chính

1. Cục Tin học và Thống kê tài chính:

a) Tham mưu cho Bộ Tài chính 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 Bộ Tài chính; Tổ chức triển khai Quy chế này và các quy định của pháp luật về an toàn an ninh mạng tại Cơ quan Bộ;

b) Tổng hợp kế hoạch, báo cáo định kỳ, đột xuất về an toàn an ninh mạng, trình Lãnh đạo Bộ Tài chính gửi các cơ quan quản lý về an toàn an ninh mạng; Xử lý các việc đột xuất về an toàn an ninh mạng (chưa quy định tại Quy chế này) theo phân công của Lãnh đạo Bộ;

c) Định kỳ hàng năm, tổ chức rà soát, kiểm tra tính phù hợp của Quy chế này với các quy định của pháp luật về an toàn thông tin mạng, an ninh mạng và các quy định, tiêu chuẩn liên quan; kiểm tra tính đáp ứng của Quy chế này với yêu cầu thực tế của Bộ Tài chính; báo cáo Bộ về việc sửa đổi, bổ sung Quy chế trong trường hợp cần thiết.

2. Tổng cục, đơn vị sự nghiệp trực thuộc Bộ:

a) Tổ chức 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; Ban hành quy định về an toàn an ninh mạng của đơn vị phù hợp với Quy chế này và các quy định của pháp luật về an toàn an ninh mạng; Xây dựng kế hoạch, báo cáo định kỳ, đột xuất về an toàn an ninh mạng và gửi Cục Tin học và Thống kê tài chính tổng hợp, báo cáo Bộ.

b) Chỉ đạo đơn vị chuyên trách an toàn an ninh mạng trực thuộc đơn vị phối hợp chặt chẽ với Cục Tin học và Thống kê tài chính trong quá trình triển khai công tác an toàn an ninh mạng tại đơn vị.

3. Cục, Vụ, đơn vị cấp tương đương trực thuộc Bộ:

a) Vụ Tổ chức cán bộ, Văn phòng Bộ, đơn vị có thẩm quyền quyết định về nhân sự có trách nhiệm bảo đảm văn bản quyết định về tiếp nhận, bổ nhiệm, điều động, chuyển công tác, thôi việc, nghỉ hưu, dừng công tác thuộc thẩm quyền phát hành của đơn vị được gửi tới Cục Tin học và Thống kê tài chính tại thời điểm phát hành văn bản.

b) 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.

c) Phối hợp với Cục Tin học và Thống kê tài chính triển khai và giám sát việc thực hiện Quy chế này tại đơn vị.

Điều 23. Trách nhiệm cá nhân thuộc Bộ Tài chính

1. Thủ trưởng đơn vị thuộc đối tượng áp dụng của Quy chế này có trách nhiệm: phổ biến tới từng cán bộ, công chức, viên chức, người lao động của đơn vị; thường xuyên kiểm tra việc thực hiện Quy chế này tại đơn vị; chịu trách nhiệm trước pháp luật và Lãnh đạo Bộ Tài chính về các vi phạm, thất thoát thông tin, dữ liệu mật thuộc phạm vi quản lý của đơn vị do không tổ chức, chỉ đạo, kiểm tra cán bộ của đơn vị thực hiện đúng quy định.

2. Cán bộ, công chức, viên chức, người lao động thuộc Bộ Tài chính, các đơn vị thuộc Bộ và các đơn vị khác thuộc đối tượng áp dụng của quy định 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. Tập thể, cá nhân vi phạm Quy chế này làm ảnh hưởng đến việc thực hiện nhiệm vụ chính trị của Bộ Tài chính 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 24. Điều khoản chuyển tiếp

Cục Tin học và Thống kê tài chính, Tổng cục phối hợp với các đơn vị liên quan rà soát hồ sơ cấp độ đã được phê duyệt; 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 12/2022/TT-BTTTT và Quy chế này (có thể phê duyệt, điều chỉnh nhiều hồ sơ đề xuất cấp độ bằng 01 quyết định phê duyệt, điều chỉnh), hoàn thành trước tháng 6 năm 2023.

Điều 25. Tổ chức thực hiện

1. Cục Tin học và Thống kê tài chính chịu trách nhiệm hướng dẫn, theo dõi, kiểm tra, đôn đốc việc thực hiện Quy chế này.

2. 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 Tin học và Thống kê tài chính để tổng hợp, báo cáo, đề xuất trình Bộ trưởng xem xét, quyết định./.

BỘ TÀI CHÍNH