| BỘ TÀI CHÍNH | CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM |
|---|---|
| | Độc lập - Tự do – Hạnh phúc |
| Số: 201 /QĐ-BTC | *Hà Nội, ngày 12 tháng 02 năm 2018* |

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

## BỘ TRƯỞNG BỘ TÀI CHÍNH

Căn cứ Luật An toàn thông tin mạng năm 2015;

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 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 Quyết định số 632/QĐ-TTg ngày 10/5/2017 của Thủ tướng Chính phủ ban hành Danh mục lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng và hệ thống thông tin quan trọng quốc gia;

Căn cứ Quyết định số 1622/QĐ-TTg ngày 25/10/2017 của Thủ tướng Chính phủ về việc phê duyệt Đề án đẩy mạnh hoạt động của mạng lưới ứng cứu sự cố, tăng cường năng lực cho cán bộ, bộ phận chuyên trách ứng cứu sự cố an toàn thông tin mạng trên toàn quốc đến 2020, định hướng đến 2025;

Căn cứ Nghị định số 87/2017/NĐ-CP ngày 26/7/2017 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Tài chính;

Căn cứ Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 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 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 Quyết định số 2582/QĐ-BKHCN ngày 25/9/2017 của Bộ trưởng Bộ Khoa học và Công nghệ về việc công bố Tiêu chuẩn quốc gia TCVN 11930:2017 yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ;

Xét 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 Bộ Tài chính.

**Điều 2.** Quyết định này có hiệu lực từ ngày ký, thay thế Quyết định số 3317/QĐ-BTC ngày 24/12/2014 của Bộ trưởng Bộ Tài chính ban hành Quy định về việc đảm bảo an toàn thông tin trên môi trường máy tính và mạng máy tính; Quyết định số 627/QĐ-BTC ngày 05/4/2017 về việc sửa đổi, bổ sung một số điều của Quy định về việc đảm bảo an toàn thông tin trên môi trường máy tính và mạng máy tính ban hành kèm theo Quyết định số 3317/QĐ-BTC ngày 24/12/2014.

**Điều 3.** Cục trưởng Cục Tin học và Thống kê tài chính, Thủ trưởng các cơ quan hành chính, đơn vị sự nghiệp, doanh nghiệp thuộc Bộ Tài chính, công chức, viên chức Bộ Tài chính, tổ chức và cá nhân 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;
- Sở Tài chính các tỉnh, thành phố;
- Cổng thông tin điện tử Bộ Tài chính;
- Lưu: VT, THTK (120b).

**KT. BỘ TRƯỞNG**
**THỨ TRƯỞNG**

**Vũ Thị Mai**

BỘ TÀI CHÍNH

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

# QUY CHẾ
## An toàn thông tin mạng Bộ Tài chính
*(Kèm theo Quyết định số 201/QĐ-BTC ngày 12 tháng 02 năm 2018 của Bộ trưởng Bộ Tài chính)*

## Chương I
## QUY ĐỊNH CHUNG

### Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. Phạm vi điều chỉnh: Quy chế này triển khai áp dụng Luật An toàn thông tin mạng, văn bản quy định, tiêu chuẩn liên quan và các biện pháp nhằm bảo đảm an toàn thông tin và các hệ thống thông tin của Bộ Tài chính.

2. Đối tượng áp dụng:

a) Cơ quan hành chính, đơn vị sự nghiệp, doanh nghiệp thuộc Bộ Tài chính (gọi chung là các đơn vị thuộc Bộ); Cán bộ thuộc các đơn vị thuộc Bộ (gọi tắt là người dùng).

b) Cơ quan, tổ chức, cá nhân có kết nối vào mạng máy tính của ngành Tài chính.

c) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ công nghệ thông tin và an toàn thông tin mạng cho các đơn vị thuộc Bộ Tài chính.

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

1. "An toàn thông tin mạng": Sự bảo vệ thông tin số và hệ thống thông tin khỏi 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.

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

3. "Mạng nội bộ": Mạng máy tính trong phạm vi trụ sở của một đơn vị thuộc Bộ.

4. "Mạng của ngành Tài chính": Từ chỉ chung "mạng nội bộ", "hạ tầng truyền thông thống nhất ngành Tài chính".

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

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

7. "Phòng chống xâm nhập": phát hiện, ngăn chặn các hoạt động vào, ra trên hệ thống thông tin được bảo vệ có dấu hiệu gây hại hoặc vi phạm chính sách an toàn mạng.

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

9. "Thiết bị HSM": Thiết bị lưu khóa bí mật và ký số chuyên dụng dùng cho cơ quan, tổ chức.

10. "Tổng cục thuộc Bộ": Kho bạc Nhà nước, Tổng cục Thuế, Tổng cục Hải quan, Tổng cục Dự trữ Nhà nước, Ủy ban Chứng khoán Nhà nước.

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

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

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

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

15. "Sở Giao dịch Chứng khoán": Sở Giao dịch Chứng khoán Hà Nội, Sở Giao dịch Chứng khoán Thành phố Hồ Chí Minh.

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

17. "Xác thực đa yếu tố": Việc kiểm tra đối tượng truy nhập hệ thống thông tin sử dụng thêm ít nhất 1 yếu tố ngoài tên truy nhập và mật khẩu.

**Điều 3. Nguyên tắc bảo đảm an toàn thông tin mạng tại Bộ Tài chính**

1. Cán bộ, công chức, viên chức, nhân viên, các đơn vị thuộc Bộ có trách nhiệm bảo đảm an toàn thông tin và hệ thống thông tin trong phạm vi xử lý công việc của mình theo quy định của Nhà nước, Bộ Tài chính và hướng dẫn của cơ quan, đơn vị có thẩm quyền trong lĩnh vực bảo đảm an toàn thông tin mạng.

2. Bảo đảm an toàn thông tin mạng phải được thực hiện tại tất cả các công đoạn liên quan đến thông tin và hệ thống thông tin.

3. Thông tin mật, thông tin thuộc Danh mục bí mật nhà nước ngành Tài chính phải được bảo vệ theo quy định của Nhà nước, quy định của Bộ Tài chính về công tác bảo vệ bí mật nhà nước và các nội dung tương ứng trong Quy chế này.

**Điều 4. Các hành vi bị nghiêm cấm**

1. Các hành vi bị nghiêm cấm quy định tại Điều 7 Luật An toàn thông tin mạng.

2. Tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập không dây của cá nhân vào mạng nội bộ; trên cùng một thiết bị thực hiện đồng thời truy cập vào mạng nội bộ và truy cập Internet bằng thiết bị kết nối Internet của cá nhân (modem quay số, USB 3G/4G, điện thoại di động, máy tính bảng, máy tính xách tay).

3. Tự ý thay đổi, gỡ bỏ biện pháp an toàn thông tin cài đặt trên thiết bị công nghệ thông tin phục vụ công việc; tự ý thay thế, lắp mới, tráo đổi thành phần của máy tính phục vụ công việc.

## Chương II
## BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN

**Điều 5. Phân định vai trò theo quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ**

1. Chủ quản hệ thống thông tin:

a) Bộ Tài chính là chủ quản hệ thống thông tin đối với các hệ thống do Bộ quyết định đầu tư hoặc Bộ được giao làm chủ đầu tư dự án xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin.

Bộ Tài chính ủy quyền cho các đơn vị thuộc Bộ quản lý trực tiếp các hệ thống do Bộ làm chủ quản thông qua một trong các văn bản sau: Quyết định phê duyệt dự án, trong đó giao đơn vị làm chủ đầu tư dự án; Thông tư của Bộ Tài chính hoặc Quyết định của Bộ trưởng Bộ Tài chính có nội dung giao đơn vị làm nhiệm vụ quản lý hệ thống; Văn bản ủy quyền theo quy định tại khoản 3 Điều 5 Thông tư số 03/2017/TT-BTTTT.

b) Các đơn vị thuộc Bộ là chủ quản hệ thống thông tin do đơn vị quyết định đầu tư dự án xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin; là chủ quản hệ thống thông tin do đơn vị phê duyệt đề cương, dự toán chi tiết; quản lý trực tiếp các hệ thống do Bộ Tài chính ủy quyền theo quy định tại điểm a khoản này.

c) Chủ quản hệ thống thông tin (hoặc đơn vị được ủy quyền quản lý trực tiếp hệ thống thông tin) thực hiện trách nhiệm theo quy định tại Điều 20 Nghị định 85/2016/NĐ-CP.

2. Đơn vị vận hành hệ thống thông tin:

a) Cục Tin học và Thống kê tài chính là đơn vị vận hành hệ thống thông tin đối với hệ thống do Cục Tin học và Thống kê tài chính làm chủ quản hoặc được Bộ Tài chính ủy quyền quản lý trực tiếp, các hệ thống do các Cục, Vụ thuộc Bộ làm chủ quản.

b) Cục Công nghệ thông tin các Tổng cục thuộc Bộ là đơn vị vận hành hệ thống thông tin do đơn vị làm chủ quản, do Tổng cục làm chủ quản hoặc được Bộ Tài chính ủy quyền quản lý trực tiếp.

c) Bộ phận chuyên trách về công nghệ thông tin thuộc doanh nghiệp (phòng Công nghệ thông tin hoặc đơn vị, bộ phận có chức năng tương đương) là đơn vị vận hành hệ thống thông tin do doanh nghiệp làm chủ quản hoặc được Bộ Tài chính ủy quyền quản lý trực tiếp.

d) Đơn vị vận hành hệ thống thông tin thực hiện trách nhiệm theo quy định tại khoản 2, 3, 4, 5 Điều 22 Nghị định 85/2016/NĐ-CP.

3. Đơn vị chuyên trách về an toàn thông tin:

a) Đơn vị vận hành hệ thống thông tin quy định tại khoản 2 điều này đồng thời đóng vai trò đơn vị chuyên trách về an toàn thông tin trong phạm vi tương ứng.

b) Đơn vị chuyên trách về an toàn thông tin cấp Bộ và Tổng cục thành lập bộ phận chuyên trách về an toàn thông tin (Phòng hoặc Tổ). Đơn vị chuyên trách về an toàn thông tin các cấp còn lại chỉ định cá nhân phụ trách (chuyên trách hoặc kiêm nhiệm) công tác an toàn thông tin mạng.

c) Đơn vị chuyên trách về an toàn thông tin thực hiện trách nhiệm theo quy định tại khoản 1 Điều 21 Nghị định 85/2016/NĐ-CP.

**Điều 6. Thẩm quyền xác định cấp độ an toàn hệ thống thông tin**

1. Đối với hệ thống đề xuất cấp độ từ 1 đến 3

a) Đề xuất cấp độ (lập hồ sơ đề xuất cấp độ):

- Đối với hệ thống phải lập dự án, chủ đầu tư chỉ đạo đơn vị lập dự án đề xuất cấp độ.

- Đối với hệ thống thuê dịch vụ, đơn vị chủ trì thuê dịch vụ đề xuất cấp độ.

- Đối với hệ thống đang trong giai đoạn triển khai, chủ quản hệ thống thông tin chỉ đạo đơn vị chủ trì triển khai hệ thống đề xuất cấp độ.

- Đối với hệ thống đang vận hành, chủ quản hệ thống thông tin chỉ đạo đơn vị vận hành hệ thống thông tin đề xuất cấp độ. Trường hợp đơn vị vận hành hệ thống thông tin ngang cấp với chủ quản hệ thống thông tin, đơn vị vận hành hệ thống thông tin phối hợp với chủ quản hệ thống thông tin đề xuất cấp độ.

b) Thẩm định, phê duyệt cấp độ:

- Đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin thực hiện thẩm định, phê duyệt hồ sơ đề xuất cấp độ đối với hệ thống thông tin được đề xuất là cấp độ 1 hoặc cấp độ 2.

- Đối với hệ thống thông tin được đề xuất là cấp độ 3: Đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin thực hiện thẩm định hồ sơ đề xuất cấp độ; Chủ quản hệ thống thông tin phê duyệt hồ sơ đề xuất cấp độ.

2. Đối với hệ thống đề xuất cấp độ 4, 5

a) Đề xuất cấp độ (lập hồ sơ đề xuất cấp độ):

- Chủ quản hệ thống thông tin (hoặc đơn vị được ủy quyền quản lý trực tiếp hệ thống thông tin) lập hồ sơ đề xuất cấp độ, trình Bộ sau khi lấy ý kiến Cục Tin học và Thống kê tài chính.

- Bộ Tài chính gửi Bộ Thông tin và Truyền thông thẩm định hồ sơ đề xuất cấp độ.

b) Thẩm định, phê duyệt cấp độ:

- Bộ Thông tin và Truyền thông chủ trì, phối hợp với Bộ Quốc phòng, Bộ Công an và các Bộ, ngành liên quan thẩm định hồ sơ đề xuất cấp độ.

- Bộ Tài chính phê duyệt hồ sơ đề xuất cấp độ đối với hệ thống thông tin cấp độ 4, phê duyệt phương án bảo đảm an toàn thông tin đối với hệ thống thông tin cấp độ 5. Chính phủ phê duyệt cấp độ đối với hệ thống cấp độ 5.

3. Cá nhân tham gia lập hồ sơ đề xuất cấp độ không được tham gia thẩm định, phê duyệt cấp độ.

**Điều 7. Căn cứ đề xuất cấp độ**

1. Cấp độ 1, 2, 3, 4 của hệ thống thông tin được đề xuất theo điểm a, b, c, d khoản 2 Điều 21 Luật An toàn thông tin mạng và Điều 7, 8, 9, 10 Nghị định 85/2016/NĐ-CP.

2. Đối với hệ thống cấp độ 5, Cục Tin học và Thống kê tài chính chủ trì, phối hợp với các đơn vị thuộc Bộ:

a) Xây dựng tiêu chí cụ thể xác định hệ thống thông tin quan trọng quốc gia thuộc lĩnh vực tài chính theo quy định tại điểm đ khoản 2 Điều 21 Luật An toàn thông tin mạng, Điều 11 Nghị định 85/2016/NĐ-CP và khoản 1 Điều 3 Quyết định số 632/QĐ-TTg; trình Bộ lấy ý kiến Bộ Thông tin và Truyền thông, Bộ Công an, Bộ Quốc phòng; hoàn thiện trình Bộ phê duyệt.

b) Trên cơ sở các tiêu chí được phê duyệt tại điểm a khoản này, xây dựng Danh mục hệ thống thông tin quan trọng quốc gia thuộc lĩnh vực tài chính; trình Bộ gửi Bộ Thông tin và Truyền thông thẩm định; hoàn thiện và trình Bộ gửi Thủ tướng Chính phủ phê duyệt.

c) Định kỳ hàng năm rà soát, đánh giá, xác định hệ thống thông tin quan trọng quốc gia thuộc lĩnh vực tài chính; đề xuất, sửa đổi bổ sung Danh mục hệ thống thông tin quan trọng quốc gia thuộc lĩnh vực tài chính trước ngày 30 tháng 11 hàng năm.

**Điều 8. Phương án bảo đảm an toàn hệ thống thông tin**

1. Nội dung phương án bảo đảm an toàn hệ thống thông tin bao gồm:

a) Các nội dung phải tuân thủ quy định của Nhà nước:

- Quản lý an toàn thông tin mạng: Chính sách chung; tổ chức, nhân sự; quản lý thiết kế, xây dựng; quản lý vận hành; kiểm tra, đánh giá và quản lý rủi ro.

- Phương án kỹ thuật: An toàn hạ tầng mạng; an toàn máy chủ; an toàn ứng dụng và an toàn dữ liệu; an toàn vật lý cho Trung tâm dữ liệu/phòng máy chủ.

b) Các nội dung phải tuân thủ Chính sách an toàn thông tin mạng Bộ Tài chính (Phụ lục 1 của Quy chế này).

c) Các nội dung phải tuân thủ quy định, chính sách của đơn vị.

2. Yêu cầu đối với phương án bảo đảm an toàn hệ thống thông tin:

a) Các nội dung tại điểm a khoản 1 điều này phải tối thiểu đáp ứng quy định tại Điều 9 Thông tư 03/2017/TT-BTTTT, tiêu chuẩn Việt Nam TCVN 11930:2017 - Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ. Các nội dung này nếu đáp ứng tiêu chuẩn TCVN 11930:2017 thì được chấp nhận đáp ứng quy định tại Thông tư 03/2017/TT-BTTTT đối với cấp độ tương ứng.

b) Trường hợp không thể đáp ứng đầy đủ yêu cầu của tiêu chuẩn Việt Nam TCVN 11930:2017, đơn vị phải giải trình lý do và đề xuất biện pháp thay thế có tác dụng tương đương (nếu có) đối với các nội dung cụ thể không đáp ứng quy định. Số lượng yêu cầu không đáp ứng không được vượt quá 05% tổng số yêu cầu của tiêu chuẩn tại cấp độ tương ứng. Các yêu cầu không đáp ứng phải nằm ngoài các yêu cầu quy định tại Thông tư 03/2017/TT-BTTT và Chính sách an toàn thông tin mạng Bộ Tài chính.

3. Đối với các hệ thống thông tin dùng chung hệ thống mạng và các giải pháp bảo vệ (các hệ thống cấp độ 1, 2, 3), phương án bảo đảm an toàn thông tin gồm 2 phần:

a) Phần dùng chung cho các hệ thống bao gồm: quản lý an toàn thông tin mạng; an toàn hạ tầng mạng; an toàn vật lý Trung tâm dữ liệu/phòng máy chủ; an toàn kết nối Internet; an toàn trong trao đổi thông tin với các tổ chức, cá nhân ngoài Bộ Tài chính; an toàn tài khoản công nghệ thông tin; an toàn máy tính phục vụ công việc; an toàn vật lý các thiết bị công nghệ thông tin.

Trong đó, phương án quản lý an toàn thông tin mạng; an toàn hạ tầng mạng; an toàn vật lý Trung tâm dữ liệu/phòng máy chủ phải đáp ứng yêu cầu

tương ứng với cấp độ cao nhất trong số các cấp độ được xác định cho các hệ thống thông tin do đơn vị quản lý và tối thiểu đáp ứng yêu cầu:

- Cấp độ 3 đối với các đơn vị cấp Trung ương gồm cơ quan Bộ Tài chính, Tổng cục thuộc Bộ, Sở Giao dịch Chứng khoán, Trung tâm Lưu ký Chứng khoán Việt Nam, Công ty Xổ số Điện toán Việt Nam.

- Cấp độ 2 đối với Cục Thuế, Cục Hải quan, Kho bạc Nhà nước tỉnh/thành phố trực thuộc Trung ương.

- Cấp độ 1 đối với Cục Dự trữ Nhà nước, Chi cục Dự trữ Nhà nước, Chi cục Hải quan, Chi cục Thuế, Kho bạc Nhà nước quận/huyện, Học viện Tài chính, các trường thuộc Bộ, Nhà xuất bản tài chính, Nhà in tài chính.

b) Phần áp dụng cho từng hệ thống thông tin cụ thể: an toàn máy chủ, an toàn ứng dụng, an toàn cơ sở dữ liệu, an toàn tài khoản công nghệ thông tin và các nội dung liên quan khác.

4. Khuyến khích các đơn vị cấp Trung ương thống nhất áp dụng phương án bảo đảm an toàn tối thiểu đáp ứng các yêu cầu của cấp độ 3 đối với tất cả các hệ thống thông tin hoạt động trên hệ thống mạng của đơn vị.

**Điều 9. Quy trình xác định cấp độ hệ thống đề xuất cấp độ 1, 2, 3**

1. Đơn vị xây dựng phương án bảo đảm an toàn thông tin mạng cho phần dùng chung cho các hệ thống thông tin của đơn vị (quy định tại điểm a khoản 3 Điều 8 của Quy chế này) theo mẫu tại Phụ lục 2. Thực hiện thẩm định và phê duyệt phương án này.

2. Nội dung đề xuất cấp độ hệ thống thông tin:

a) Xác định và phân loại hệ thống thông tin theo khoản 2 Điều 6 Nghị định 85/2016/NĐ-CP và Điều 4 Thông tư 03/2017/TT-BTTTT.

b) Xác định chủ quản hệ thống thông tin, đơn vị vận hành hệ thống thông tin theo khoản 1, 2 Điều 5 của Quy chế.

c) Xác định loại thông tin được xử lý thông qua hệ thống thông tin theo khoản 1 Điều 6 Nghị định 85/2016/NĐ-CP.

d) Thuyết minh về việc đề xuất cấp độ theo Điều 7 của Quy chế.

đ) Thuyết minh phương án bảo đảm an toàn thông tin theo cấp độ tương ứng, gồm các phần sau:

- Tham chiếu phương án bảo đảm an toàn thông tin mạng dùng chung cho các hệ thống thông tin trong phạm vi đơn vị.

- Thuyết minh phương án bảo đảm an toàn thông tin áp dụng riêng cho hệ thống thông tin được đề xuất cấp độ.

3. Đối với dự án đầu tư xây dựng mới hoặc mở rộng, nâng cấp hệ thống thông tin:

a) Nội dung đề xuất cấp độ được lồng ghép (bổ sung chương, mục) vào thiết kế sơ bộ của báo cáo nghiên cứu khả thi, dự án khả thi ứng dụng công nghệ thông tin hoặc báo cáo đầu tư của dự án.

b) Thẩm định:

- Việc thẩm định đề xuất cấp độ được thực hiện đồng thời với quá trình thẩm định thiết kế sơ bộ.

- Đơn vị thẩm định đề xuất cấp độ gửi kết quả thẩm định cho đơn vị thẩm định dự án để tổng hợp, báo cáo cấp có thẩm quyền phê duyệt dự án.

4. Đối với hệ thống thông tin đang trong giai đoạn triển khai chưa xác định cấp độ

a) Nội dung đề xuất cấp độ được lồng ghép (bổ sung chương, mục) vào tài liệu thiết kế thi công đối với hệ thống thông tin lập dự án hoặc lập thành tài liệu độc lập đối với hệ thống thông tin không lập dự án.

b) Thẩm định:

- Việc thẩm định đề xuất cấp độ được thực hiện đồng thời với quá trình thiết kế thi công hoặc triển khai hệ thống.

- Đơn vị thẩm định đề xuất cấp độ gửi kết quả thẩm định cho đơn vị thẩm định thiết kế thi công để tổng hợp, báo cáo cấp có thẩm quyền phê duyệt thiết kế thi công.

5. Đối với hệ thống thông tin đang vận hành chưa xác định cấp độ

a) Hồ sơ đề xuất cấp độ cho một hệ thống thông tin theo mẫu tại Phụ lục 3. Hồ sơ đề xuất cấp độ cho nhiều hệ thống thông tin theo mẫu tại Phụ lục 4.

b) Hồ sơ đề xuất cấp độ có thể được lập và phê duyệt dưới dạng điện tử (có chữ ký số của lãnh đạo hoặc chữ ký số của đơn vị đề xuất và phê duyệt hồ sơ). Khuyến khích đơn vị áp dụng hồ sơ điện tử.

6. Tổ chức xác định cấp độ trong nội bộ đơn vị

a) Bộ phận được giao chủ trì đề xuất, xây dựng, triển khai hệ thống thông tin (thuộc chủ quản hệ thống thông tin hoặc đơn vị vận hành hệ thống thông tin) phối hợp với bộ phận chuyên trách về an toàn thông tin của đơn vị chuyên trách về an toàn thông tin xây dựng đề xuất cấp độ; xây dựng phương án bảo đảm an toàn thông tin cho hệ thống; lập hồ sơ đề xuất cấp độ cho hệ thống; đồng trình hồ sơ đề xuất cấp độ lên lãnh đạo đơn vị vận hành hệ thống thông tin (theo mẫu văn bản tờ trình áp dụng trong nội bộ đơn vị).

b) Bộ phận chuyên trách về an toàn thông tin chịu trách nhiệm quản lý toàn bộ các hồ sơ đề xuất cấp độ an toàn thông tin đã được phê duyệt.

**Điều 10. Quy trình xác định cấp độ hệ thống đề xuất cấp độ 4, 5**

1. Hồ sơ đề xuất cấp độ đối với hệ thống đề xuất cấp độ 4, 5 thực hiện theo quy định tại Điều 15 Nghị định 85/2016/NĐ-CP; Điều 7 và điểm b khoản 4

Điều 8 Thông tư 03/2017/TT-BTTTT và hướng dẫn bổ sung của Bộ Thông tin và Truyền thông (nếu có).

2. Quy trình thẩm định, phê duyệt hồ sơ đề xuất cấp độ 4, 5 theo khoản 2 Điều 6 của Quy chế.

**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, phải rà soát cấp độ, phương án bảo đảm an toàn của hệ thống và thực hiện điều chỉnh, bổ sung hoặc thay mới hồ sơ đề xuất cấp độ trong trường hợp cần thiết.

**Điều 12. Triển khai phương án bảo đảm an toàn hệ thống thông tin**

1. Chủ quản hệ thống thông tin hoặc đơn vị được ủy quyền quản lý trực tiếp hệ thống thông tin tổ chức triển khai phương án bảo đảm an toàn hệ thống thông tin sau khi hồ sơ đề xuất cấp độ hoặc phương án bảo đảm an toàn hệ thống được phê duyệt.

2. Bộ phận chuyên trách về an toàn thông tin thuộc đơn vị chịu trách nhiệm giám sát việc triển khai các phương án bảo đảm an toàn thông tin đã được phê duyệt (trên cơ sở lập hồ sơ theo dõi từng hệ thống thông tin theo mẫu tham khảo tại Phụ lục 5 của Quy chế).

## Chương III
## GIÁM SÁT, CẢNH BÁO AN TOÀN THÔNG TIN MẠNG

**Điều 13. Giám sát an toàn thông tin mạng**

1. Đối tượng giám sát bắt buộc: Hệ thống thông tin từ cấp độ 3 trở lên.

2. Thời gian giám sát tối thiểu: Giám sát 24 giờ/ngày và 7 ngày/tuần đối với hệ thống cấp độ 4, 5; Giám sát trong giờ làm việc đối với hệ thống cấp độ 3.

3. Nội dung, phương thức, hệ thống kỹ thuật phục vụ công tác giám sát: Thực hiện theo quy định tại Điều 5 Thông tư số 31/2017/TT-BTTTT.

**Điều 14. Cảnh báo an toàn thông tin mạng**

1. Đơn vị chuyên trách về an toàn thông tin cử 01 lãnh đạo đơn vị chuyên trách an toàn thông tin và 01 cán bộ thuộc bộ phận chuyên trách về an toàn thông tin 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.

Đầu mối tiếp nhận cảnh báo phân tích sơ bộ mức độ ảnh hưởng tới các hệ thống thông tin của đơn vị mình, chuyển tiếp cảnh báo cho các bộ phận liên quan xử lý, tổng hợp và gửi báo cáo kết quả xử lý cho đầu mối tiếp nhận cảnh

báo của Cục Tin học và Thống kê tài chính qua thư điện tử hoặc điện thoại hoặc bằng văn bản trong trường hợp được yêu cầu báo cáo bằng văn bản.

2. Đơn vị chuyên trách về an toàn thông tin 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 thông tin 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 Bộ Công an, Bộ Thông tin và Truyền thông, 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.

## Chương IV
## ỨNG CỨU SỰ CỐ AN TOÀN THÔNG TIN MẠNG

### Điều 15. Nội dung ứng cứu sự cố an toàn thông tin mạng

1. Sự cố an toàn thông tin mạng bao gồm:

a) Sự cố do bị tấn công mạng: tấn công từ chối dịch vụ; tấn công giả mạo; tấn công sử dụng mã độc; truy cập trái phép, chiếm quyền điều khiển; tấn công thay đổi giao diện; tấn công mã hóa phần mềm, dữ liệu, thiết bị; phá hoại thông tin, dữ liệu, phần mềm; nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu; các hình thức tấn công mạng khác.

b) Hỏng hóc phần cứng, lỗi phần mềm của hệ thống thông tin làm mất tính sẵn sàng của hệ thống thông tin.

c) Hỏng hóc, lỗi của các hệ thống thuộc hạ tầng Trung tâm dữ liệu, phòng máy chủ (nguồn điện, làm mát, chống sét, chống cháy...) làm mất tính sẵn sàng của hệ thống thông tin.

d) Hỏng hóc, lỗi của hệ thống mạng làm mất khả năng truy cập tới hệ thống thông tin của các đối tượng sử dụng hệ thống.

đ) Sự cố do lỗi của người quản trị, vận hành hệ thống.

e) Sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn.

2. Hoạt động ứng cứu sự cố an toàn thông tin mạng huy động các nguồn lực nằm ngoài phạm vi của đơn vị vận hành hệ thống thông tin để đối phó với các sự cố quy định tại khoản 1 điều này.

**Điều 16. Phân định vai trò theo quy định của pháp luật về ứng cứu sự cố an toàn thông tin mạng**

1. Ban Chỉ đạo ứng cứu sự cố an toàn thông tin mạng Bộ Tài chính do Ban Chỉ đạo ứng dụng công nghệ thông tin Bộ Tài chính đảm nhiệm. Ban Chỉ đạo ứng cứu sự cố an toàn thông tin mạng Bộ Tài chính thực hiện trách nhiệm theo quy định tại khoản 2 Điều 5 Quyết định số 05/2017/QĐ-TTg.

2. Đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng

a) Cục Tin học và Thống kê tài chính đảm nhiệm vai trò Đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng Bộ Tài chính, chịu trách nhiệm quản lý (hướng dẫn, tổng hợp, giám sát, kiểm tra) công tác ứng cứu sự cố an toàn thông tin mạng toàn ngành Tài chính và trực tiếp triển khai công tác ứng cứu sự cố các hệ thống thông tin tại cơ quan Bộ Tài chính, các hệ thống thông tin dùng chung toàn ngành do Cục quản lý.

b) Cục Công nghệ thông tin các Tổng cục thuộc Bộ, Trung tâm thông tin Học viện Tài chính, Sở Giao dịch Chứng khoán, Trung tâm Lưu ký Chứng khoán Việt Nam, Công ty Xổ số điện toán Việt Nam đảm nhiệm vai trò chuyên trách về ứng cứu sự cố an toàn thông tin mạng trong phạm vi quản lý công nghệ thông tin của đơn vị.

c) Đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng thực hiện trách nhiệm quy định tại khoản 2 Điều 6 Quyết định số 05/2017/QĐ-TTg.

3. Đội ứng cứu sự cố an toàn thông tin mạng

a) Các đơn vị chuyên trách về ứng cứu sự cố quy định tại khoản 2 điều này thành lập Đội ứng cứu sự cố thuộc đơn vị.

b) Thành phần Đội ứng cứu sự cố bao gồm:

- Đội trưởng: Lãnh đạo đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng.

- Đội phó gồm: 01 đội phó thường trực là lãnh đạo phòng/phụ trách nhóm Quản lý an toàn an ninh thông tin (hoặc tương đương), 01 đội phó là lãnh đạo phòng/phụ trách nhóm Quản trị, vận hành hệ thống (hoặc tương đương), 01 đội phó là lãnh đạo/phụ trách nhóm Quản lý phát triển ứng dụng (hoặc tương đương).

- Thành viên: cán bộ thuộc các phòng/trung tâm/bộ phận làm công tác quản lý an toàn an ninh thông tin; quản trị, vận hành hệ thống; quản lý phát triển ứng dụng; và các bộ phận liên quan khác tùy theo đặc thù của từng đơn vị.

c) Đội ứng cứu sự cố có trách nhiệm phối hợp với các bên liên quan phân tích, xử lý sự cố an toàn thông tin mạng đối với các sự cố diễn ra trong phạm vi hệ thống thuộc quản lý của chủ quản hệ thống thông tin.

**Điều 17. Tham gia mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia**

1. Thành viên có nghĩa vụ phải tham gia mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia theo quy định tại điểm a, đ khoản 1 Điều 7 Quyết định số 05/2017/QĐ-TTg: Cục Tin học và Thống kê tài chính; các Cục Công nghệ thông tin thuộc Kho bạc Nhà nước, Tổng cục Thuế, Tổng cục Hải quan.

2. Thành viên tự nguyện tham gia mạng lưới: Khuyến khích các đơn vị thuộc Bộ không thuộc quy định tại khoản 1 điều này và đáp ứng 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. Đơn vị được Cơ quan điều phối quốc gia chấp thuận tham gia mạng lưới phải thông báo cho Cục Tin học và Thống kê tài chính.

3. Các đơn vị tham gia mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia thực hiện trách nhiệm theo quy định tại khoản 4 Điều 7 Quyết định số 05/2017/QĐ-TTg và các quy định đối với thành viên mạng lưới tại Thông tư số 20/2017/TT-BTTTT.

**Điều 18. Liên minh ứng cứu sự cố an toàn thông tin mạng**

1. Liên minh ứng cứu sự cố: tập hợp toàn bộ các đơn vị tham gia công tác ứng cứu sự cố an toàn thông tin mạng của một đơn vị; bao gồm tất cả các đối tác có liên quan đến việc đảm bảo sự hoạt động bình thường của hệ thống thông tin và hiểu rõ về hệ thống (đối tác xây dựng ứng dụng, cung cấp thiết bị/đường truyền, cung cấp giải pháp/dịch vụ an toàn thông tin...); có thể có sự tham gia của các đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng quốc gia (VNCERT, Trung tâm Internet Việt Nam, Cục Cảnh sát phòng, chống tội phạm công nghệ cao…).

2. Cục Tin học và Thống kê tài chính, các Tổng cục thuộc Bộ, các Sở Giao dịch Chứng khoán, Trung tâm Lưu ký Chứng khoán Việt Nam, Công ty Xổ số Điện toán Việt Nam hình thành Liên minh ứng cứu sự cố để thực hiện ứng cứu các hệ thống thông tin do đơn vị trực tiếp quản lý. Trách nhiệm của từng thành viên trong Liên minh được quy định tại các điều khoản về hỗ trợ xử lý sự cố/hỗ trợ kỹ thuật/ứng cứu sự cố trong các hợp đồng kinh tế, các thỏa thuận hợp tác song phương hoặc các quy định của Nhà nước về ứng cứu sự cố (đối với các thành viên tham gia mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia); các thành viên tham gia Liên minh được liệt kê đầy đủ trong Kế hoạch ứng phó sự cố an toàn thông tin của mỗi đơn vị.

3. Vai trò của các bên tham gia Liên minh ứng cứu sự cố

a) Đơn vị vận hành hệ thống thông tin đóng vai trò chủ trì, điều phối trong Liên minh ứng cứu sự cố.

b) Các đơn vị nghiệp vụ tham gia trong việc xây dựng kịch bản xử lý nghiệp vụ trong trường hợp hệ thống thông tin xảy ra sự cố nghiêm trọng.

c) Các đơn vị tham gia Liên minh ứng cứu sự cố có nghĩa vụ chia sẻ thông tin, phối hợp xử lý sự cố theo sự điều phối của đơn vị chủ trì Liên minh.

**Điều 19. Kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng**

1. Cục Tin học và Thống kê tài chính, các Tổng cục thuộc Bộ, Học viện Tài chính, các Sở Giao dịch Chứng khoán, Trung tâm Lưu ký Chứng khoán Việt Nam, Công ty Xổ số Điện toán Việt Nam tổ chức xây dựng, phê duyệt Kế hoạch ứng phó sự cố cho các hệ thống thông tin do đơn vị trực tiếp quản lý theo đề cương tại Phụ lục II Quyết định số 05/2017/QĐ-TTg (bao gồm các điều chỉnh do Bộ Thông tin và Truyền thông ban hành nếu có) và tổ chức triển khai kế hoạch sau khi phê duyệt. Đối với các nội dung trong kế hoạch vượt thẩm quyền quyết định của đơn vị, đơn vị lấy ý kiến của Cục Tin học và Thống kê tài chính, Cục Kế hoạch - Tài chính (đối với các nội dung yêu cầu có kinh phí), báo cáo Bộ xem xét, quyết định.

2. Các kế hoạch ứng phó sự cố sau khi được phê duyệt phải gửi Cục Tin học và Thống kê tài chính tổng hợp thành kế hoạch chung toàn ngành. Cục Tin học và Thống kê tài chính có trách nhiệm xây dựng Kế hoạch ứng phó sự cố chung toàn ngành, trình Lãnh đạo Bộ Tài chính phê duyệt.

3. Kế hoạch ứng phó sự cố được rà soát và điều chỉnh hàng năm (nếu cần thiết) trước ngày 31 tháng 10, làm cơ sở để xây dựng kế hoạch bảo đảm an toàn thông tin năm tiếp theo.

**Điều 20. Quy trình ứng cứu sự cố an toàn thông tin mạng**

1. Quy trình ứng cứu sự cố nghiêm trọng

a) Đối tượng áp dụng quy trình: Đơn vị quản lý trực tiếp hệ thống thông tin cấp độ 4, 5.

b) Nội dung quy trình: theo quy định tại Điều 14 Quyết định 05/2017/QĐ-TTg.

c) Trong quá trình ứng cứu sự cố, đơn vị chuyên trách ứng cứu sự cố cung cấp thông tin diễn biến tình hình cho Cục Tin học và Thống kê tài chính nắm thông tin và phối hợp xử lý; Chủ quản hệ thống thông tin báo cáo tình hình cho Lãnh đạo Bộ.

2. Quy trình ứng cứu sự cố không nghiêm trọng

a). Đối tượng áp dụng: Chủ quản hệ thống thông tin, đơn vị vận hành hệ thống thông tin.

b) Nội dung quy trình: theo quy định tại Điều 11 Thông tư 20/2017/TT-BTTTT.

c) Đối với các báo cáo phải gửi Cơ quan điều phối quốc gia về ứng cứu sự cố an toàn thông tin mạng, chủ quản hệ thống thông tin gửi một bản cho Cục Tin học và Thống kê tài chính theo dõi.

**Điều 21. Thông báo, báo cáo sự cố an toàn thông tin mạng**

1. 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 điểm a khoản 1 Điều 11 Quyết định 05/2017/QĐ-TTg và Điều 9 Thông tư 20/2017/TT-BTTT, đồng thời báo cáo Cục Tin học và Thống kê tài chính để Cục tổng hợp, báo cáo Ban Chỉ đạo ứng cứu sự cố an toàn thông tin mạng Bộ Tài chính.

2. Đơn vị phải thông báo trong toàn đơn vị 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 hoặc sự cố an toàn thông tin mạng liên quan đến các hệ thống thông tin do đơn vị quản lý.

**Điều 22. Diễn tập ứng cứu sự cố**

a) Chủ quản hệ thống thông tin tổ chức diễn tập ứng cứu sự cố theo Kế hoạch ứng phó sự cố được phê duyệt.

b) Cục Tin học và Thống kê tài chính chủ trì, phối hợp với các đơn vị thuộc Bộ tham gia các cuộc diễn tập quốc gia, quốc tế do Cơ quan điều phối quốc gia, Bộ Thông tin và Truyền thông tổ chức và tổ chức diễn tập ứng cứu sự cố trong phạm vi Bộ Tài chính theo tần suất quy định tại điểm b Nhiệm vụ 4 mục II Điều 1 Quyết định số 1622/QĐ-TTg ngày 25/10/2017 của Thủ tướng Chính phủ.

## Chương V

## ĐÀO TẠO, BỒI DƯỠNG NGHIỆP VỤ, TUYÊN TRUYỀN, PHỔ BIẾN, NÂNG CAO NHẬN THỨC VỀ AN TOÀN THÔNG TIN MẠNG

**Điều 23. Đối tượng đào tạo, bồi dưỡng về an toàn thông tin mạng**

1. Người sử dụng máy tính (cán bộ nghiệp vụ, hành chính tại các đơn vị thuộc Bộ) được đào tạo kiến thức cơ bản về an toàn thông tin mạng, hướng dẫn sử dụng các ứng dụng an toàn.

2. Cán bộ quản lý.

3. Cán bộ công nghệ thông tin.

4. Cán bộ chuyên trách công tác an toàn thông tin mạng.

**Điều 24. Trách nhiệm tổ chức đào tạo, bồi dưỡng về an toàn thông tin mạng**

1. Cục Tin học và Thống kê tài chính tổ chức đào tạo, bồi dưỡng nghiệp vụ về an toàn thông tin cho cán bộ công nghệ thông tin, cán bộ chuyên trách an toàn thông tin mạng các đơn vị hành chính thuộc Bộ; đào tạo cơ bản về an toàn thông tin cho cán bộ quản lý, người sử dụng máy tính cơ quan Bộ Tài chính.

2. Các Tổng cục thuộc Bộ tổ chức đào tạo, bồi dưỡng nghiệp vụ về an toàn thông tin cho cán bộ công nghệ thông tin, cán bộ chuyên trách an toàn thông tin mạng các đơn vị thuộc Tổng cục; đào tạo cơ bản về an toàn thông tin cho cán bộ quản lý, người sử dụng máy tính thuộc đơn vị.

3. Các doanh nghiệp, đơn vị sự nghiệp tổ chức đào tạo cho nhân viên thuộc đơn vị mình.

## Chương VI

## BÁO CÁO, CHIA SẺ THÔNG TIN VỀ AN TOÀN THÔNG TIN MẠNG

### Điều 25. Chế độ báo cáo

1. Báo cáo định kỳ:

a) Báo cáo an toàn thông tin định kỳ hàng năm gồm các nội dung quy định tại khoản 3 Điều 17 Thông tư 03/2017/TT-BTTTT.

b) Báo cáo hoạt động giám sát của chủ quản hệ thống thông tin định kỳ 6 tháng theo mẫu tại Phụ lục 2 Thông tư 31/2017/TT-BTTTT.

2. Báo cáo đột xuất: Báo cáo về công tác khắc phục mã độc, lỗ hổng, điểm yếu, triển khai cảnh báo an toàn thông tin và các báo cáo đột xuất khác theo yêu cầu của các cơ quan quản lý nhà nước về an toàn thông tin.

3. Trách nhiệm lập, phê duyệt báo cáo

a) Các Tổng cục, đơn vị sự nghiệp, doanh nghiệp thuộc Bộ chịu trách nhiệm:

- Lập báo cáo an toàn thông tin theo quy định tại điểm a khoản 1 điều này, gửi Cục Tin học và Thống kê tài chính trước ngày 15 tháng 11 hàng năm.

- Lập báo cáo hoạt động giám sát của chủ quản hệ thống thông tin theo quy định tại điểm b khoản 1 điều này, gửi Cục Tin học và Thống kê tài chính trước ngày 15 tháng 6 và 15 tháng 12 hàng năm.

- Báo cáo đột xuất theo hướng dẫn của Cục Tin học và Thống kê tài chính.

b) Cục Tin học và Thống kê tài chính chịu trách nhiệm tập hợp, tổng hợp báo cáo của các đơn vị, trình Bộ phê duyệt, gửi các cơ quan quản lý nhà nước về an toàn thông tin.

### Điều 26. Chia sẻ thông tin

1. Việc chia sẻ thông tin về công tác bảo đảm an toàn thông tin với các đơn vị ngoài Bộ được thực hiện theo quy định tại Điều 18 Thông tư 03/2017/TT-BTTT.

2. Khuyến khích các đơn vị thuộc Bộ chia sẻ kinh nghiệm triển khai, vận hành hệ thống an toàn thông tin thông qua trao đổi trực tiếp giữa các đơn vị hoặc hội thảo nội bộ Bộ Tài chính.

3. Cục Tin học và Thống kê tài chính chịu trách nhiệm tổ chức hội thảo trao đổi kinh nghiệm giữa các đơn vị thuộc Bộ tối thiểu 2 năm 1 lần.

## Chương VII
## KIỂM TRA, ĐÁNH GIÁ VỀ AN TOÀN THÔNG TIN MẠNG

### Điều 27. Kiểm tra việc tuân thủ quy định về an toàn thông tin và hiệu quả của biện pháp bảo đảm an toàn thông tin

1. Nội dung kiểm tra, đánh giá

a) Kiểm tra việc xác định cấp độ an toàn hệ thống thông tin và triển khai phương án bảo đảm an toàn thông tin; Kiểm tra hiệu quả của các biện pháp bảo đảm an toàn thông tin.

b) Kiểm tra công tác giám sát an toàn thông tin; ứng cứu sự cố an toàn thông tin.

c) Kiểm tra các nội dung khác tại Quy chế.

2. Thẩm quyền kiểm tra

a) Cục Tin học và Thống kê tài chính chịu trách nhiệm kiểm tra các Tổng cục, doanh nghiệp, đơn vị sự nghiệp thuộc Bộ.

b) Các đơn vị tự kiểm tra trong nội bộ đơn vị.

3. Kỳ kiểm tra:

a) Cục Tin học và Thống kê tài chính kiểm tra định kỳ 02 năm đối với các Tổng cục, doanh nghiệp, đơn vị sự nghiệp thuộc Bộ.

b) Các Tổng cục kiểm tra định kỳ hàng năm trong nội bộ đơn vị.

4. Hoạt động kiểm tra về an toàn thông tin do Cục Tin học và Thống kê tài chính thực hiện tại các Tổng cục thuộc chương trình kiểm tra công tác ứng dụng công nghệ thông tin hàng năm, theo kế hoạch được Bộ Tài chính phê duyệt. Hoạt động kiểm tra về an toàn thông tin do các Tổng cục thuộc Bộ thực hiện có thể lồng ghép trong chương trình kiểm tra công tác ứng dụng công nghệ thông tin hàng năm, theo kế hoạch được Lãnh đạo đơn vị phê duyệt.

### Điều 28. Đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống

Hoạt động đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thực hiện theo quy định tại điểm c khoản 2 Điều 20 Nghị định số 85/2016/NĐ-CP và Điều 13 Thông tư số 03/2017/TT-BTTTT.

**Điều 29. Đánh giá tổng thể an toàn thông tin**

1. Nội dung đánh giá: Đánh giá công tác bảo đảm an toàn thông tin mạng theo tiêu chuẩn Việt Nam (TCVN ISO/IEC 27000, TCVN 11930) hoặc tiêu chuẩn quốc tế (COBIT, NIST, ISO/IEC 27000), khung đánh giá an toàn thông tin của các tổ chức an toàn thông tin khác).

2. Phương thức đánh giá: Đơn vị tự tổ chức đánh giá hoặc thuê tổ chức được cấp phép cung cấp dịch vụ an toàn thông tin mạng thực hiện đánh giá theo kỳ đánh giá quy định tại điểm c khoản 2 Điều 20 Nghị định 85/2017/NĐ-CP.

## Chương VIII
## TRÁCH NHIỆM ĐỐI VỚI CÔNG TÁC AN TOÀN THÔNG TIN MẠNG

**Điều 30. Trách nhiệm của các đơn vị thuộc Bộ**

1. Cục Tin học và Thống kê tài chính:

a) Thực hiện các trách nhiệm được giao tại Quy chế này.

b) Hướng dẫn triển khai Quy chế này và các quy định liên quan của Nhà nước.

c) Tổ chức triển khai thực hiện Quy chế tại trụ sở cơ quan Bộ Tài chính.

d) Xây dựng kế hoạch, báo cáo về an toàn thông tin mạng của Bộ Tài chính.

2. Các Tổng cục thuộc Bộ:

a) Thực hiện các trách nhiệm được giao tại Quy chế này.

b) Tổ chức triển khai thực hiện Quy chế này tại đơn vị.

c) Thực hiện các báo cáo theo quy định, gửi Cục Tin học và Thống kê tài chính tổng hợp, báo cáo Bộ.

3. Các Cục, Vụ thuộc Bộ:

a) Thực hiện trách nhiệm của chủ quản hệ thống thông tin trong trường hợp có hệ thống thông tin thuộc quản lý trực tiếp của đơn vị theo quy định của Quy chế này.

b) Phối hợp với Cục Tin học và Thống kê tài chính triển khai Quy chế này tại đơn vị.

4. Các đơn vị sự nghiệp, doanh nghiệp thuộc Bộ:

a) Thực hiện trách nhiệm của chủ quản hệ thống thông tin hoặc đơn vị quản lý trực tiếp hệ thống thông tin trong trường hợp có hệ thống thông tin thuộc quản lý trực tiếp của đơn vị theo quy định của Quy chế này.

b) Tổ chức triển khai thực hiện Quy chế này tại đơn vị.

c) Thực hiện các báo cáo về an toàn thông tin mạng khi được Bộ Tài chính yêu cầu.

5. Các đơn vị vận hành hệ thống thông tin:

a) Thực hiện trách nhiệm của đơn vị vận hành hệ thống thông tin theo quy định tại Quy chế này và các nhiệm vụ do chủ quản hệ thống thông tin phân công.

b) Chỉ đạo, phân công các bộ phận kỹ thuật thuộc đơn vị (quản lý ứng dụng; quản lý dữ liệu; vận hành hệ thống thông tin; triển khai và hỗ trợ kỹ thuật) triển khai công tác bảo đảm an toàn thông tin trong tất cả các công đoạn liên quan đến hệ thống thông tin.

6. Các đơn vị chuyên trách về an toàn thông tin của các đơn vị thuộc Bộ:

a) Thực hiện trách nhiệm của đơn vị chuyên trách về an toàn thông tin theo quy định tại Quy chế này và các nhiệm vụ do chủ quản hệ thống thông tin phân công.

b) Phối hợp chặt chẽ với các bộ phận kỹ thuật thuộc đơn vị vận hành hệ thống thông tin trong việc bảo đảm an toàn thông tin trong tất cả các công đoạn liên quan đến hệ thống thông tin.

7. Cơ quan, tổ chức, cá nhân ngoài ngành Tài chính có liên quan: Tuân thủ Quy chế này, quy định công tác bảo vệ bí mật nhà nước của ngành Tài chính, các cam kết, thỏa thuận với các đơn vị thuộc Bộ Tài chính về đảm bảo an toàn thông tin khi cung cấp dịch vụ công nghệ thông tin và thực hiện các hoạt động trao đổi thông tin với các đơn vị thuộc Bộ. Trường hợp tham gia sử dụng ứng dụng của ngành Tài chính, phải tuân thủ các yêu cầu, hướng dẫn, quy trình đảm bảo an toàn thông tin cụ thể của ứng dụng.

**Điều 31. Trách nhiệm cá nhân**

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, nhân viên 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, nhân viên của 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 thông tin cho đơn vị, bộ phận chuyên trách về an toàn thông tin mạng của đơn vị; 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 bảo đảm an toàn thông tin mạng Bộ Tài chính 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.

## Chương IX
## TỔ CHỨC THỰC HIỆN

### Điều 32. Tổ chức triển khai Quy chế

1. Cục Tin học và Thống kê tài chính, các Tổng cục, đơn vị sự nghiệp, doanh nghiệp thuộc Bộ xây dựng Kế hoạch triển khai Quy chế theo mẫu tại Phụ lục 6, đảm bảo đến năm 2020 tất cả các hệ thống thông tin thuộc quản lý của đơn vị được phê duyệt hồ sơ đề xuất cấp độ, triển khai đầy đủ hoạt động giám sát an toàn thông tin, ứng cứu sự cố an toàn thông tin và các hoạt động khác theo quy định tại Quy chế này; gửi Cục Tin học và Thống kê tài chính Kế hoạch triển khai Quy chế trong vòng 45 ngày kể từ ngày Quy chế này có hiệu lực.

2. Cục Tin học và Thống kê tài chính tổng hợp kế hoạch của các đơn vị, tổ chức thảo luận với các đơn vị, thống nhất thành kế hoạch chung của Bộ Tài chính, trình Bộ phê duyệt, làm căn cứ để giám sát và đôn đốc tiến độ triển khai Quy chế của các đơn vị.

3. Các đơn vị rà soát kế hoạch triển khai Quy chế theo định kỳ hàng năm, gửi kế hoạch điều chỉnh (nếu có) cho Cục Tin học và Thống kê tài chính kèm theo Báo cáo an toàn thông tin định kỳ hàng năm.

### Điều 33. Rà soát, cập nhật, bổ sung Quy chế

Hàng năm, Cục Tin học và Thống kê tài chính tổ chức rà soát, kiểm tra tính phù hợp của Quy chế này với các quy định của Nhà nước về bảo đảm an toàn thông tin mạng và các quy định, tiêu chuẩn liên quan, kiểm tra tính đáp ứng của Quy chế này (bao gồm Chính sách an toàn thông tin mạng Bộ Tài chính) với yêu cầu thực tế của Bộ Tài chính; báo cáo Bộ về việc cập nhật, bổ sung Quy chế trong trường hợp cần thiết./.

**KT. BỘ TRƯỞNG**
**THỨ TRƯỞNG**

**Vũ Thị Mai**

## Phụ lục 1. Chính sách an toàn thông tin mạng Bộ Tài chính

### 1. Bảo đảm an toàn kết nối Internet

1.1. Mục đích kết nối, truy cập Internet:

a) Hệ thống thông tin được thiết lập kết nối Internet cho các mục đích:

- Cung cấp thông tin; cung cấp dịch vụ công trực tuyến, các dịch vụ trong phạm vi quy định của pháp luật.

- Kết nối tới hệ thống thông tin của các cơ quan, tổ chức để phục vụ hoạt động nghiệp vụ, trao đổi thông tin, phối hợp cung cấp dịch vụ công trực tuyến.

- Cung cấp cổng truy cập ứng dụng nội bộ cho cán bộ từ Internet.

- Cập nhật phiên bản phần mềm, bản vá phần mềm; Cập nhật mẫu mã độc, mẫu tấn công.

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

1.2. Cách thức thiết lập kết nối Internet:

a) Hệ thống thông tin khi kết nối Internet phải thông qua kiểm soát của tường lửa và hệ thống bảo vệ kết nối truy cập Internet.

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

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

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

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

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

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

1.4. Kết nối Internet cho máy tính phục vụ công việc của người dùng tại đơn vị bị thu hẹp phạm vi hoặc bị ngắt trong các trường hợp sau:

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

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

1.5. Các biện pháp kỹ thuật bảo đảm an toàn kết nối, truy cập Internet:

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

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

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

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

d) Truy cập mạng, ứng dụng nội bộ từ Internet phải thực hiện xác thực đa yếu tố.

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

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

**2. Bảo đảm an toàn trong hoạt động trao đổi thông tin với các tổ chức, cá nhân ngoài Bộ Tài chính**

2.1. Đối với cơ quan, tổ chức, cá nhân ngoài Bộ Tài chính có thiết lập kết nối vào hệ thống mạng của ngành Tài chính:

Vùng mạng của tổ chức, cá nhân bên ngoài được sử dụng để kết nối vào mạng của ngành Tài chính phải được kiểm soát bằng tường lửa; các máy tính trong phân đoạn mạng này phải được cập nhật bản vá hệ điều hành, mẫu phòng diệt mã độc; các tài khoản truy cập hệ thống tối thiểu phải áp dụng mật khẩu

phức tạp; chỉ được kết nối Internet trong trường hợp kết nối này phục vụ trực tiếp công việc của các đơn vị thuộc Bộ và đáp ứng quy định về bảo đảm an toàn kết nối Internet tại đơn vị.

2.2. Đối tác phát triển ứng dụng cho các đơn vị thuộc Bộ Tài chính có trách nhiệm đảm bảo an toàn cho công tác phát triển ứng dụng, bao gồm cả giai đoạn bảo trì, bảo hành ứng dụng: sử dụng máy tính được cập nhật bản vá hệ điều hành, phần mềm phòng diệt mã độc; thực hiện các biện pháp tránh lộ lọt mã nguồn, phần mềm ứng dụng của ngành Tài chính và các tài liệu liên quan; không sử dụng các công cụ phát triển ứng dụng không có bản quyền hoặc có nguồn gốc không an toàn.

2.3. Các đối tác cung cấp dịch vụ công nghệ thông tin (bao gồm thử nghiệm sản phẩm công nghệ thông tin tại hệ thống mạng của đơn vị thuộc Bộ) và nhân viên của đối tác trong trường hợp tiếp xúc với bí mật nhà nước của ngành Tài chính phải ký cam kết bảo vệ bí mật nhà nước trước khi triển khai hợp đồng, thỏa thuận về dịch vụ công nghệ thông tin.

**3. Bảo đảm an toàn tài khoản công nghệ thông tin**

3.1. Tài khoản người dùng:

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

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

c) Trường hợp người dùng thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ hưu phải thông báo kịp thời cho bộ phận quản lý tài khoản công nghệ thông tin để thực hiện điều chỉnh, thu hồi, hủy bỏ các quyền sử dụng của người dùng đối với hệ thống mạng, ứng dụng. Quy định cụ thể như sau:

- Văn bản quyết định về việc bổ nhiệm chức vụ lãnh đạo, thay đổi vị trí công tác, chuyển công tác, thôi việc, nghỉ hưu phải ghi tên bộ phận chịu trách nhiệm quản lý tài khoản công nghệ thông tin tại phần ghi nơi nhận của văn bản. Trường hợp thay đổi vị trí công tác không sử dụng hình thức văn bản quyết định, đơn vị quản lý người dùng phải thông báo cho bộ phận quản lý tài khoản công nghệ thông tin bằng công văn hoặc theo cách thức quy định trong quy trình quản lý tài khoản công nghệ thông tin áp dụng tại đơn vị.

- Tài khoản công nghệ thông tin phải được điều chỉnh, thu hồi, hủy bỏ trong thời gian không quá 03 ngày làm việc tính từ ngày người dùng chính thức chuyển công tác ra khỏi ngành Tài chính, thôi việc, nghỉ hưu; không quá 05

ngày làm việc trong trường hợp thay đổi vị trí công tác trong nội bộ đơn vị hoặc chuyển công tác tới đơn vị khác thuộc ngành Tài chính.

- Phải có văn bản đề nghị của đơn vị quản lý người dùng trong trường hợp cần duy trì tài khoản của người dùng sau thời điểm người dùng chính thức thay đổi vị trí công tác, chuyển công tác, thôi việc, nghỉ hưu; trong đó nêu rõ lý do, các quyền sử dụng cần duy trì và thời gian duy trì.

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

3.3. Xác thực tài khoản công nghệ thông tin:

a) Mật khẩu truy cập, sử dụng, quản trị hệ thống thông tin; truy cập thiết bị lưu khóa bí mật phải:

- 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.

b) Mật khẩu phải được đổi ngay sau khi nhận bàn giao từ người khác hoặc có thông báo về sự cố an toàn thông tin, điểm yếu liên quan đến khả năng lộ mật khẩu; mật khẩu phải được đổi tối thiểu 03 tháng một lần đối với tài khoản của người dùng và 02 tháng một lần đối với tài khoản quản trị hệ thống.

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

3.4. Hệ thống tài khoản công nghệ thông tin phải được rà soát hàng năm, đảm bảo các tài khoản và quyền truy cập hệ thống được cấp phát đúng. Các tài khoản không sử dụng trong thời gian 01 năm phải bị khóa hoặc xóa bỏ (sau khi trao đổi, xác nhận với đơn vị sử dụng).

**4. Bảo đảm an toàn máy tính phục vụ công việc**

4.1. Máy tính phục vụ công việc (bao gồm máy chủ, máy tính quản trị và máy tính để bàn, máy tính xách tay, máy tính bảng phục vụ công việc của người dùng tại đơn vị):

a) Máy tính phục vụ công việc chỉ được cài đặt phần mềm theo danh mục phần mềm do đơn vị quy định và do đơn vị/bộ phận chuyên trách về công nghệ thông tin của đơn vị quản lý hoặc được cung cấp theo các chương trình ứng dụng công nghệ thông tin của Bộ Tài chính và các cơ quan Nhà nước khác có

thẩm quyền, được cập nhật bản vá lỗi hệ điều hành về an ninh, cài đặt phần mềm phòng diệt mã độc và cập nhật mẫu mã độc hàng ngày.

b) Đơn vị/bộ phận chuyên trách về công nghệ thông tin của đơn vị chịu trách nhiệm cài đặt phần mềm cho máy tính phục vụ công việc. Người dùng không được can thiệp vào các phần mềm đã cài đặt trên máy tính (thay đổi, gỡ bỏ,...) khi chưa được sự đồng ý của bộ phận công nghệ thông tin của đơn vị.

4.2. Máy tính do cá nhân tự trang bị phải đáp ứng đầy đủ các điều kiện dưới đây khi kết nối vào hệ thống mạng của ngành Tài chính:

a) Cài đặt đầy đủ các bản vá lỗi hệ điều hành về an ninh.

b) Cài đặt phần mềm phòng diệt mã độc và cập nhật mẫu mã độc gần nhất.

c) Không cài đặt phần mềm, công cụ có tính năng gây mất an toàn thông tin hoặc tạo rủi ro cho hệ thống mạng (cấp phát địa chỉ mạng, dò quét mật khẩu, dò quét cổng mạng, giả lập tấn công,..).

d) Được sự kiểm tra và đồng ý của bộ phận quản lý Công nghệ thông tin của đơn vị hoặc đáp ứng yêu cầu của hệ thống kiểm tra tự động trên cơ sở đối chiếu với các quy định tại điểm a, b, c của khoản này.

**5. Bảo đảm an toàn vật lý các thiết bị công nghệ thông tin**

5.1. Các khu vực sau phải được kiểm soát truy cập vật lý để phòng tránh truy cập trái phép hoặc sai mục đích: Trung tâm dữ liệu; khu vực chứa máy chủ và thiết bị lưu trữ; tủ mạng và đấu nối; thiết bị nguồn điện và dự phòng điện khẩn cấp; phòng vận hành, kiểm soát, quản trị hệ thống. Phải có nội quy hoặc hướng dẫn làm việc trong các khu vực này.

5.2. Các điểm truy cập không dây của đơn vị được bảo vệ tránh bị tiếp cận trái phép.

5.3. Máy chủ, thiết bị mạng trung tâm phải được đặt tại Trung tâm dữ liệu hoặc phòng máy chủ.

5.4. Thiết bị thuộc hệ thống thông tin từ cấp độ 2 trở lên phải được bảo dưỡng định kỳ và duy trì chế độ bảo hành liên tục hoặc có cơ chế sửa chữa, thay thế đáp ứng yêu cầu về mức độ sẵn sàng của hệ thống thông tin trong suốt thời gian sử dụng.

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

5.6. Người dùng sử dụng các thiết bị lưu trữ dữ liệu di động (máy tính xách tay, thiết bị số cầm tay, thẻ nhớ USB, ổ cứng ngoài, băng từ) để xử lý công việc của cơ quan có trách nhiệm bảo vệ các thiết bị này và thông tin lưu trên

thiết bị, tránh làm mất, lộ thông tin; xóa ngay thông tin lưu trữ trên thiết bị sau khi hoàn thành xử lý. Không mang ra nước ngoài thông tin của cơ quan, Nhà nước không liên quan tới nội dung công việc thực hiện ở nước ngoài. Người dùng sử dụng các thiết bị lưu trữ dữ liệu di động do đơn vị cấp phát không tự ý thuê, mua dịch vụ sao lưu, phục hồi dữ liệu khi gặp sự cố hỏng hóc mà báo bộ phận Công nghệ thông tin của đơn vị để xử lý; không tự ý hủy các thiết bị này khi không còn khả năng sử dụng.

5.7. Người dùng phải thực hiện thao tác khoá máy tính (sử dụng tính năng có sẵn trên máy) khi rời khỏi nơi đặt máy tính; tắt máy tính khi rời khỏi cơ quan.

**Phụ lục 2. Mẫu thuyết minh phương án bảo đảm an toàn thông tin mạng dùng chung cho các hệ thống thông tin**

1. Cấp độ đề xuất: ….

2. Đối chiếu với Tiêu chuẩn TCVN 11930:2017 cấp độ .... (tương ứng với cấp độ đề xuất tại mục 1)

| Yêu cầu của TCVN 11930:2017 | Hiện trạng | Phương án cải thiện hiện trạng | Đánh giá đáp ứng tiêu chuẩn | Lý do, biện pháp thay thế đối với các nội dung không đáp ứng tiêu chuẩn |
|---|---|---|---|---|
| X.1 Yêu cầu quản lý | | | | |
| … | | | | |
| X.2 Yêu cầu kỹ thuật | | | | |
| X.2.1 Bảo đảm an toàn mạng | | | | |
| … | | | | |
| A.Y Yêu cầu vật lý | | | | |
| … | | | | |

3. Đối chiếu với chính sách an toàn thông tin mạng Bộ Tài chính

| Chính sách của Bộ Tài chính | Hiện trạng | Phương án cải thiện hiện trạng | Đánh giá đáp ứng tiêu chuẩn | Lý do, biện pháp thay thế đối với các nội dung không đáp ứng chính sách |
|---|---|---|---|---|
| 1. Bảo đảm an toàn kết nối Internet | | | | |
| ... | | | | |
| 2. Bảo đảm an toàn trong hoạt động trao đổi thông tin với các tổ chức, cá nhân ngoài Bộ Tài chính | | | | |
| ... | | | | |

| | | | | |
|---|---|---|---|---|
| 3. Bảo đảm an toàn tài khoản công nghệ thông tin | | | | |
| ... | | | | |
| 4. Bảo đảm an toàn máy tính phục vụ công việc | | | | |
| ... | | | | |
| 5. Bảo đảm an toàn vật lý các thiết bị công nghệ thông tin | | | | |
| ... | | | | |

4. Đối chiếu với quy định, chính sách của đơn vị

| Quy định, chính sách của đơn vị | Hiện trạng | Phương án cải thiện hiện trạng | Đánh giá đáp ứng tiêu chuẩn | Lý do, biện pháp thay thế đối với các nội dung không đáp ứng quy định |
|---|---|---|---|---|
| | | | | |
| | | | | |

*Ghi chú: Có thể ghép các bảng tại mục 2, 3, 4 vào chung thành một bảng nếu phù hợp.*

## Phụ lục 3. Mẫu Hồ sơ đề xuất cấp độ an toàn hệ thống thông tin

### Tài liệu 1: THUYẾT MINH ĐỀ XUẤT CẤP ĐỘ VÀ PHƯƠNG ÁN BẢO ĐẢM AN TOÀN THÔNG TIN

1. Tên hệ thống thông tin

2. Mô tả chung về hệ thống thông tin

2.1 Chức năng chính của hệ thống thông tin

2.2 Đối tượng sử dụng:

2.3 Mô hình hệ thống thông tin:

2.4 Hệ điều hành và các phần mềm CSDL, ứng dụng sử dụng cho hệ thống thông tin:

3. Phân loại hệ thống thông tin (theo khoản 2 Điều 5 Nghị định 85/2016/NĐ-CP và Điều 4 Thông tư 03/2017/TT-BTTTT):

4. Chủ quản hệ thống thông tin (theo khoản 1, 2 Điều 5 của Quy chế):

5. Đơn vị vận hành hệ thống thông tin (theo khoản 1, 2 Điều 5 của Quy chế):

6. Loại thông tin được xử lý thông qua hệ thống thông tin (theo khoản 1 Điều 6 Nghị định 85/2016/NĐ-CP):

7. Cấp độ đề xuất (kèm thuyết minh căn cứ đề xuất cấp độ (theo Điều 7 của Quy chế):

8. Thuyết minh phương án bảo đảm an toàn thông tin (tương ứng với cấp độ đề xuất)

8.1 Phương án bảo đảm an toàn thông tin mạng dùng chung

Tham chiếu Quyết định phê duyệt phương án bảo đảm an toàn thông tin mạng dùng chung nếu đã có quyết định này hoặc mô tả phương án bảo đảm bảo đảm an toàn thông tin mạng dùng chung.

8.2 Phương án bảo đảm an toàn áp dụng cho mỗi hệ thống thông tin

8.2.1 Đối chiếu với Tiêu chuẩn TCVN 11930:2017

| Yêu cầu của TCVN 11930:2017 cấp độ.. | Hiện trạng | Phương án cải thiện hiện trạng | Đánh giá đáp ứng tiêu chuẩn | Lý do, biện pháp thay thế đối với các nội dung không đáp ứng yêu cầu |
|---|---|---|---|---|
| | | | | |
| | | | | |

8.2.2 Đối chiếu với quy định, chính sách của đơn vị (có thể ghép chung với bảng tại mục 8.2.1 nếu phù hợp).

**Tài liệu 2:** Tài liệu mô tả chi tiết hệ thống (Thiết kế sơ bộ hoặc Thiết kế thi công hoặc Tài liệu hoàn công).

## Phụ lục 4. Mẫu Hồ sơ đề xuất cấp độ áp dụng cho nhiều hệ thống thông tin

**1. Đề xuất cấp độ**

| TT | Tên hệ thống | Mô tả chung hệ thống | Phân loại hệ thống | Loại thông tin xử lý trên hệ thống | Chủ quản hệ thống thông tin | Đơn vị vận hành | Cấp độ đề xuất | Thuyết minh đề xuất cấp độ |
|---|---|---|---|---|---|---|---|---|
| 1 | | | | | | | | |
| 2 | | | | | | | | |

**2. Phương án bảo đảm an toàn thông tin**

2.1 Phương án bảo đảm an toàn thông tin mạng dùng chung

Tham chiếu Quyết định phê duyệt phương án bảo đảm an toàn thông tin mạng dùng chung nếu đã có quyết định này hoặc mô tả phương án bảo đảm bảo đảm an toàn thông tin mạng dùng chung.

2.2 Phương án bảo đảm an toàn áp dụng cho mỗi hệ thống thông tin

2.2.1 Hệ thống thông tin 1 – *Tên hệ thống* – Cấp độ đề xuất:

2.2.2.1 Đối chiếu với Tiêu chuẩn TCVN 11930:2017

| Yêu cầu của Tiêu chuẩn TCVN 11930:2017 | Hiện trạng | Phương án cải thiện hiện trạng | Đánh giá đáp ứng tiêu chuẩn | Lý do, biện pháp thay thế đối với các nội dung không đáp ứng yêu cầu |
|---|---|---|---|---|
| | | | | |
| | | | | |

2.2.2.2 Đối chiếu với quy định, chính sách của đơn vị (có thể ghép chung với bảng tại mục 2.2.2.1 nếu phù hợp).

2.2.2 Hệ thống thông tin 2 – *Tên hệ thống* – Cấp độ đề xuất:

.....

**Phụ lục 5. Mẫu tham khảo Hồ sơ theo dõi triển khai phương án bảo đảm an toàn cho hệ thống thông tin**

1. Tên Hệ thống thông tin:
2. Cấp độ đề xuất được phê duyệt:
3. Cấp độ phương án bảo đảm an toàn thông tin đề xuất được phê duyệt:

| Yêu cầu của Tiêu chuẩn TCVN 11930:2017/Quy định, chính sách của đơn vị | Hiện trạng | Phương án cải thiện hiện trạng | Đánh giá đáp ứng tiêu chuẩn | Lý do, biện pháp thay thế đối với các nội dung không đáp ứng yêu cầu | Tiến độ triển khai phương án bảo đảm an toàn thông tin |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |

**Phụ lục 6. Mẫu Kế hoạch triển khai Quy chế An toàn thông tin mạng Bộ Tài chính**

**KẾ HOẠCH TRIỂN KHAI QUY CHẾ AN TOÀN THÔNG TIN MẠNG BỘ TÀI CHÍNH ĐẾN NĂM 2020**

**I. Xác định cấp độ an toàn thông tin**

1. Phân công vai trò, trách nhiệm trong hoạt động xác định cấp độ an toàn thông tin

2. Xác định cấp độ đối với phần dùng chung cho các hệ thống của đơn vị (*xem điểm a khoản 3 Điều 8 của Quy chế*):

- Cấp độ dự kiến:....

- Kế hoạch xây dựng chính sách quản lý an toàn thông tin mạng tương ứng với cấp độ dự kiến theo Tiêu chuẩn TCVN 11930:2017 (*dự kiến thời gian hoàn thành xây dựng mới hoặc rà soát, hoàn thiện các quy định hiện có của đơn vị*):

- Kế hoạch rà soát, hoàn thiện hệ thống mạng, Trung tâm dữ liệu/phòng máy chủ và các nội dung khác của phần dùng chung.

3. Xác định cấp độ cho các hệ thống thông tin

| TT | Tên hệ thống | Tình trạng<br>*(đang hoạt động/chuẩn bị lập dự án/đang triển khai)* | Cấp độ dự kiến<br>*(theo thứ tự từ cao xuống thấp)* | Dự kiến thời gian xác định cấp độ<br>*(quý/năm - quý/năm)* |
|---|---|---|---|---|
| A | Các hệ thống phục vụ người dân, doanh nghiệp, đối tượng quản lý, đối tượng phục vụ | | | |
| ... | | | | |
| B | Các hệ thống phục vụ nội bộ | | | |
| .. | | | | |
| C | Các hệ thống hạ tầng | | | |
| ... | | | | |
| D | Các hệ thống điều khiển công nghiệp và hệ thống khác | | | |

**II. Giám sát an toàn thông tin**

1. Hiện trạng hoạt động giám sát an toàn thông tin

2. Kế hoạch triển khai hoạt động giám sát an toàn thông tin

**III. Ứng cứu sự cố an toàn thông tin mạng**

| TT | Công việc | Thời gian dự kiến triển khai (*quý/năm*) |
|---|---|---|
| 1 | Đăng ký tham gia mạng lưới ứng cứu sự cố | |
| 2 | Thành lập đội ứng cứu sự cố | |
| 3 | Xây dựng Kế hoạch ứng phó sự cố | |
| 4 | Thành lập Liên minh ứng cứu sự cố | |

**IV. Đào tạo, bồi dưỡng nghiệp vụ về an toàn thông tin**

1. Tình hình công tác đào tạo, bồi dưỡng nghiệp vụ về an toàn thông tin của đơn vị đến thời điểm này

2. Định hướng triển khai công tác đào tạo, bồi dưỡng về nghiệp vụ an toàn thông tin của đơn vị từ năm 2018-2020

**V. Kiểm tra, đánh giá an toàn thông tin**

1. Tình hình công tác tự kiểm tra, đánh giá an toàn thông tin tính đến thời này

2. Dự kiến triển khai công tác kiểm tra, đánh giá an toàn thông tin từ năm 2018-2020