| BỘ TƯ PHÁP<br>------- | CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM<br>Độc lập - Tự do - Hạnh phúc<br>---------- |
|---|---|
| Số: 45/QĐ-BTP | *Hà Nội, ngày 16 tháng 01 năm 2023* |



# QUYẾT ĐỊNH

BAN HÀNH QUY CHẾ BẢO ĐẢM AN TOÀN, AN NINH THÔNG TIN MẠNG BỘ TƯ PHÁP

## BỘ TRƯỞNG BỘ TƯ PHÁP

*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 98/2022/NĐ-CP ngày 29/11/2022 của Chính phủ quy định về chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Tư pháp;*

*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 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ về Quy định chi tiết một số điều của Luật An ninh mạng;*

*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 Công nghệ thông tin.*

## QUYẾT ĐỊNH:

**Điều 1.** Ban hành kèm theo Quyết định này Quy chế Bảo đảm an toàn, an ninh thông tin mạng Bộ Tư pháp.

**Điều 2.** Quyết định này có hiệu lực kể từ ngày ký và thay thế Quyết định số 299/QĐ-BTP ngày 08/02/2014 của Bộ trưởng Bộ Tư pháp về ban hành Quy chế Quản lý, vận hành, khai thác, sử dụng và bảo đảm an toàn thông tin hệ thống mạng máy tính của Bộ Tư pháp.

**Điều 3.** Cục trưởng Cục Công nghệ thông tin, Chánh Văn phòng Bộ, Vụ trưởng Vụ Tổ chức cán bộ, Cục trưởng Cục Kế hoạch - Tài chính, Thủ trưởng các đơn vị và cá nhân có liên quan thuộc Bộ Tư pháp chịu trách nhiệm thi hành Quyết định này./.

**KT. BỘ TRƯỞNG**
**THỨ TRƯỞNG**

***Nơi nhận:***
- Như điều 3;
- Bộ trưởng Lê Thành Long (để b/c);
- Các Thứ trưởng (để biết);
- Lưu: VT, Cục CNTT.

**Nguyễn Khánh Ngọc**

# QUY CHẾ

BẢO ĐẢM AN TOÀN, AN NINH THÔNG TIN MẠNG BỘ TƯ PHÁP

*(Ban hành kèm theo Quyết định số 45/QĐ-BTP ngày 16 tháng 01 năm 2023 của Bộ trưởng Bộ Tư pháp)*

## Chương I

## NHỮNG QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh: Quy chế này quy định về việc bảo đảm an toàn, an ninh thông tin mạng trong các hoạt động của Bộ Tư pháp.

2. Đối tượng áp dụng:

a) Các đơn vị thuộc Bộ Tư pháp và cán bộ, công chức, viên chức và người lao động thuộc các đơn vị thuộc Bộ.

b) Cơ quan, tổ chức, cá nhân có hoạt động, thiết bị kết nối vào hệ thống mạng của Bộ Tư pháp.

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

### Điều 2. Giải thích từ ngữ

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

1. *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.

2. *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.

3. *Hạ tầng kỹ thuật* là tập hợp các thiết bị tính toán (máy chủ, máy trạm), lưu trữ, thiết bị ngoại vi, thiết bị kết nối mạng, thiết bị phụ trợ, đường truyền, mạng nội bộ, mạng diện rộng ...

4. *Phần mềm độc hại* là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

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.

### Điều 3. Nguyên tắc bảo đảm an toàn, an ninh thông tin

1. Bảo đảm an toàn, an ninh thông tin là yêu cầu bắt buộc, thường xuyên, liên tục, có tính xuyên suốt quá trình liên quan đến thông tin và thiết kế, xây dựng, vận hành, nâng cấp, hủy bỏ hệ thống thông tin. Bảo đảm an toàn, an ninh thông tin tuân thủ các nguyên tắc chung quy định tại Luật An toàn thông tin mạng, Luật An ninh mạng, Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ về Quy định chi tiết một số điều của Luật An ninh mạng (gọi tắt là Nghị định số 53/2022/NĐ-CP) và 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 (gọi tắt là Nghị định số 85/2016/NĐ-CP) và các quy định pháp luật khác có liên quan.

2. Xác định rõ quyền hạn, trách nhiệm của Thủ trưởng đơn vị, từng bộ phận, cá nhân trong đơn vị đối với công tác bảo đảm an ninh, an toàn thông tin. Các đơn vị bố trí nhân sự làm đầu mối phối hợp với Cục Công nghệ thông tin trong việc bảo đảm an toàn, an ninh thông tin.

3. Tuân thủ các quy định và hướng dẫn về bảo đảm an toàn, an ninh thông tin của cơ quan có thẩm quyền.

4. Cán bộ, công chức, viên chức và người lao động trong các đơn vị thuộc Bộ có trách nhiệm bảo đảm an toàn, an ninh thông tin trong phạm vi xử lý công việc của mình theo quy định của Nhà nước và của Bộ Tư pháp.

5. Thông tin có bí mật nhà nước phải được bảo vệ theo các quy định pháp luật về bí mật nhà nước; Quy chế bảo vệ bí mật nhà nước của Bộ Tư pháp và các nội dung tương ứng trong Quy chế này.

6. Xử lý sự cố an toàn, an ninh thông tin phải phù hợp với trách nhiệm, quyền hạn và bảo đảm lợi ích hợp pháp của cơ quan, đơn vị, cá nhân liên quan và theo quy định của pháp luật.

**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, Điều 8 Luật An ninh mạng và Điều 5 Luật Bảo vệ bí mật nhà nước.

2. Tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập mạng không dây của cá nhân vào các mạng máy tính của cơ quan mà không có sự đồng ý bằng văn bản của đơn vị quản lý.

3. Tự ý kết nối máy tính cá nhân với hệ thống mạng của Bộ Tư pháp (trừ hệ thống mạng không dây quản lý tập trung của Bộ).

4. Tự ý kết nối máy tính soạn thảo tài liệu mật với các thiết bị có tính năng lưu trữ, thiết bị có tính năng thu phát sóng, thiết bị có tính năng truyền dữ liệu (thiết bị lưu trữ USB thương mại, thẻ nhớ, máy tính bảng, máy ảnh, điện thoại di động, thiết bị thu phát sóng 3G/4G ...), ngoại trừ trường hợp sử dụng thiết bị chuyên dụng do Ban Cơ yếu Chính phủ sản xuất.

5. Nghiêm cấm chuyển đổi mục đích sử dụng từ máy tính dùng để soạn thảo, lưu trữ thông tin mật có nội dung bí mật nhà nước sang máy tính có kết nối Internet và ngược lại mà chưa có giải pháp hủy dữ liệu triệt để.

6. Sử dụng chung thiết bị có tính năng lưu trữ tài liệu (thiết bị lưu trữ USB, thẻ nhớ, ổ cứng rời ...) trên máy tính ở các mạng khác nhau trong Bộ Tư pháp (như mạng vùng quản trị, vùng cơ sở dữ liệu, vùng ra internet...).

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

8. Tạo ra, cài đặt, phát tán phần mềm độc hại gây ảnh hưởng đến hoạt động bình thường của hệ thống thông tin, hệ thống mạng Bộ Tư pháp

9. Cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin; ngăn chặn việc truy nhập đến thông tin của cơ quan, cá nhân khác trên môi trường mạng, trừ trường hợp pháp luật cho phép.

10. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của cơ quan, cá nhân khác trên môi trường mạng.

11. Tự ý chia sẻ thông tin tài khoản và mật khẩu của đơn vị, cá nhân trái quy định, thẩm quyền.

12. Các hành vi khác làm mất an toàn, bí mật thông tin của cơ quan, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

**Chương II**

## QUY ĐỊNH BẢO ĐẢM AN TOÀN, AN NINH THÔNG TIN MẠNG

**Điều 5. Xác định cấp độ và phương án bảo đảm an toàn, an ninh hệ thống thông tin. Xác lập hệ thống thông tin quan trọng về an ninh quốc gia**

1. Việc xác định cấp độ hệ thống thông tin và xây dựng phương án bảo vệ hệ thống thông tin theo cấp độ phục vụ mục đích đánh giá an toàn thông tin và bảo đảm an toàn thông tin cho các hệ thống thông tin. Nguyên tắc bảo đảm an toàn thông tin theo cấp độ và nguyên tắc xác định cấp độ căn cứ trên các nguyên tắc quy định tại Điều 4, Điều 5 Nghị định 85/2016/NĐ-CP.

2. Chủ quản hệ thống thông tin

a) Bộ Tư pháp 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 nhiệm vụ, dự án xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin.

Bộ Tư pháp 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 loại văn bản sau: Quyết định phê duyệt dự án, trong đó giao đơn vị làm chủ đầu tư dự án; Quyết định của Bộ trưởng Bộ Tư pháp có nội dung giao đơn vị làm nhiệm vụ quản lý hệ thống; Văn bản ủy quyền theo quy định tại 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 (sau đây gọi tắt là Thông tư số 12/2022/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, quyết định giao kinh phí thường xuyên để 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 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.

3. Đơn vị vận hành hệ thống thông tin

a) Đơn vị vận hành hệ thống thông tin được quy định tại Điều 5 Thông tư số 12/2022/TT-BTTTT.

b) Đơn vị vận hành hệ thống thông tin là đơn vị được Bộ giao chủ quản hệ thống thông tin.

4. Đơn vị chuyên trách về an toàn, an ninh thông tin mạng

Cục Công nghệ thông tin là đơn vị chuyên trách về an toàn thông tin mạng và an ninh mạng của Bộ Tư pháp.

5. Trình tự, thủ tục, thẩm quyền xác định cấp độ an toàn hệ thống thông tin

a) Đơn vị lập hồ sơ đề xuất cấp độ:

- Đối với các hệ thống thông tin thuộc các nhiệm vụ, dự án đang trong giai đoạn lập dự án, đơn vị lập dự án lập hồ sơ đề xuất cấp độ;

- Đối với các hệ thống thông tin thuê dịch vụ, đơn vị chủ trì thuê dịch vụ lập hồ sơ đề xuất cấp độ;

- Đối với các hệ thống thông tin đang trong giai đoạn triển khai, đơn vị chủ trì triển khai lập hồ sơ đề xuất cấp độ;

- Đối với các hệ thống thông tin đang vận hành, đơn vị vận hành lập hồ sơ đề xuất cấp độ.

- Việc xác định, phân loại hệ thống thông tin theo quy định tại Thông tư số 12/2022/TT-BTTTT

- Nội dung của hồ sơ đề xuất cấp độ hệ thống thông tin theo quy định tại Điều 15 Nghị định 85/2016/NĐ-CP.

- Nội dung, thời gian thẩm định hồ sơ đề xuất cấp độ hệ thống thông tin quy định tại Điều 16 Nghị định 85/2016/NĐ-CP.

- Trình tự, thủ tục xác định cấp độ hệ thống thông tin theo quy định tại Điều 13, Điều 14 Nghị định 85/2016/NĐ-CP và Điều 07, Điều 08 Thông tư số 12/2022/TT-BTTTT.

b) Đối với các hệ thống thông tin được đề xuất từ cấp độ 3 trở lên, đơn vị cần gửi xin ý kiến chuyên môn của Cục Công nghệ thông tin trước khi trình các cấp có thẩm quyền thẩm định, phê duyệt cấp độ.

c) Thẩm quyền thẩm định và phê duyệt cấp độ theo quy định tại Thông tư số 12/2022/TT-BTTTT .

6. Phương án bảo đảm an toàn hệ thống thông tin

a) Phương án bảo đảm an toàn hệ thống thông tin phải phù hợp với cấp độ của hệ thống thông tin và đáp ứng yêu cầu quy định tại Thông tư số 12/2022/TT-BTTTT , phù hợp với tiêu chuẩn TCVN 11930:2017 , các tiêu chuẩn, quy chuẩn kỹ thuật khác và chính sách an toàn thông tin mạng của Bộ Tư pháp.

b) 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.

c) Đơn vị chuyên trách chịu trách nhiệm giám sát việc triển khai các phương án bảo đảm an toàn thông tin đã được phê duyệt.

7. Hàng năm, chủ quản hệ thống thông tin có trách nhiệm rà soát, đối chiếu với quy định tại khoản 4 Điều 3 Nghị định 53/2022/NĐ-CP để lập hồ sơ đề nghị đưa hệ thống thông tin thuộc thẩm quyền quản lý của mình vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

**Điều 6. Bảo đảm an toàn, an ninh thông tin trong quản lý tài sản CNTT**

1. Phân loại tài sản CNTT:

a) Tài sản phần cứng (vật lý): là các trang thiết bị phần cứng CNTT, phương tiện truyền thông và các trang thiết bị phục vụ cho hoạt động của hệ thống thông tin;

b) Tài sản phần mềm: là các phần mềm hệ thống, phần mềm thương mại, phần mềm nội bộ, phần mềm ứng dụng, cơ sở dữ liệu và công cụ phát triển phần mềm;

c) Tài sản thông tin: là các thông tin, cơ sở dữ liệu, dữ liệu ở dạng số hóa.

2. Yêu cầu về quản lý tài sản CNTT:

a) Giao, gắn trách nhiệm cho cá nhân hoặc tập thể quản lý, sử dụng tài sản CNTT.

b) Quy định các quy tắc sử dụng, giữ gìn bảo vệ tài sản CNTT trong các trường hợp như: mang ra khỏi cơ quan, trang thiết bị CNTT liên quan đến dữ liệu bảo mật, thông tin cài đặt và cấu hình.

c) Tài sản phần cứng có lưu trữ dữ liệu quan trọng khi thay đổi mục đích sử dụng hoặc thanh lý, đơn vị phải phối hợp với bộ phận chuyên trách về CNTT thực hiện các biện pháp xóa, tiêu hủy dữ liệu đó bảo đảm không có khả năng phục hồi. Trường hợp không thể tiêu hủy được dữ liệu, đơn vị phải thực hiện tiêu hủy cấu phần lưu trữ dữ liệu trên trang thiết bị CNTT đó.

d) Trang thiết bị CNTT có bộ phận lưu trữ dữ liệu hoặc thiết bị lưu trữ dữ liệu khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài hoặc ngừng sử dụng phải tháo bộ phận lưu trữ khỏi thiết bị (bắt buộc thực hiện đối với trường hợp thiết bị có liên quan dữ liệu mật) hoặc xóa thông tin, dữ liệu lưu trữ trên thiết bị (trừ trường hợp để khôi phục dữ liệu).

đ) Các đơn vị có trách nhiệm bảo dưỡng, bảo trì và hướng dẫn cách sử dụng, quản lý, vận hành hệ thống hạ tầng kỹ thuật của mình; chỉ định bộ phận thực hiện quản lý, vận hành và định kỳ kiểm tra, sửa chữa, bảo trì thiết bị (bao gồm thiết bị đang hoạt động và thiết bị dự phòng).

**Điều 7. Bảo đảm an toàn về mặt vật lý và môi trường nơi lắp đặt trang thiết bị tại Trung tâm dữ liệu điện tử**

1. Các thiết bị kết nối mạng, thiết bị bảo mật quan trọng như tường lửa (firewall), thiết bị định tuyến (router), hệ thống máy chủ, hệ thống lưu trữ SAN, NAS,... phải được đặt trong trung tâm dữ liệu điện tử của Bộ và phải được thiết lập cơ chế bảo vệ, theo dõi phát hiện xâm nhập và biện pháp kiểm soát truy cập, kết nối vật lý phù hợp với từng khu vực: máy chủ và hệ thống lưu trữ; tủ mạng và đầu nối; thiết bị nguồn điện và dự phòng điện khẩn cấp; vận hành, kiểm soát, quản trị hệ thống. Cục Công nghệ thông tin quản lý Trung tâm dữ liệu điện tử của Bộ (TTDLĐT) có trách nhiệm xây dựng nội quy hoặc hướng dẫn làm việc tại TTDLĐT.

2. Trung tâm dữ liệu điện tử của Bộ là khu vực hạn chế tiếp cận. Chỉ những cá nhân có quyền, nhiệm vụ theo phân công của thủ trưởng đơn vị mới được phép vào TTDLĐT. Việc vào, ra TTDLĐT phải được kiểm soát bằng thiết bị bảo vệ (quẹt thẻ, vân tay, nhận dạng sinh trắc học ...).

3. Trung tâm dữ liệu điện tử của Bộ phải được trang bị hệ thống lưu điện đủ công suất và duy trì thời gian hoạt động của các máy chủ ít nhất 30 phút khi có sự cố mất điện.

4. Trung tâm dữ liệu điện tử của Bộ phải có hệ thống làm mát điều hòa không khí, độ ẩm để bảo đảm môi trường vận hành; hệ thống cảnh báo cháy, hệ thống chữa cháy tự động bằng khí, thiết bị phòng cháy, chữa cháy khẩn cấp; hệ thống cảnh báo hệ thống nguồn điện; hệ thống chống sét lan truyền. Các hệ thống này phải được thiết lập chế độ cảnh báo phù hợp. Cục Công nghệ thông tin phải cử cán bộ thường xuyên giám sát thiết bị, hạ tầng của trung tâm dữ liệu điện tử của Bộ.

**Điều 8. Khai thác, sử dụng hệ thống mạng máy tính của Bộ Tư pháp**

1. Cục Công nghệ thông tin áp dụng các biện pháp kỹ thuật cần thiết để bảo đảm hoạt động kết nối Internet của người dùng tại đơn vị được an toàn và thông suốt. Tối thiểu đáp ứng các yêu cầu sau: có hệ thống tường lửa và hệ thống bảo vệ truy cập Internet, đáp ứng nhu cầu kết nối đồng thời, hỗ trợ các công nghệ mạng riêng ảo thông dụng và khả năng bảo vệ hệ thống trước các loại tấn công từ chối dịch vụ; lọc bỏ, không cho phép truy cập các trang tin có nghi ngờ chứa mã độc hoặc các nội dung không phù hợp; thực hiện đăng ký để cấp phát địa chỉ mạng cho thiết bị lần đầu trên hệ thống để cho phép kết nối mạng.

2. Các đơn vị khi có nhu cầu kết nối trang thiết bị vào hệ thống mạng máy tính của Bộ Tư pháp với mục đích phục vụ công việc, có trách nhiệm thông báo bằng công văn cho Cục Công nghệ thông tin để phối hợp thực hiện việc kết nối vào mạng máy tính của Bộ.

3. Các đơn vị và cá nhân tham gia vào hệ thống mạng máy tính không được tự ý thay đổi những thông số mạng hay tự ý đưa các thiết bị mạng, thiết bị viễn thông khác tham gia kết nối vào hệ thống mạng.

4. Các cơ quan bên ngoài khi có kết nối trực tiếp vào mạng của Bộ Tư pháp phải được sự đồng ý của Cục Công nghệ thông tin và tuân theo các quy định, các tiêu chuẩn kỹ thuật phù hợp với hệ thống mạng của Bộ Tư pháp.

5. Các đơn vị và cá nhân sẽ được cấp tài khoản của đơn vị và người dùng để truy cập vào các hệ thống thông tin và hệ thống mạng máy tính của Bộ Tư pháp thực hiện nhiệm vụ.

6. Các cá nhân không được sử dụng hệ thống mạng máy tính của Bộ để khai thác, lưu trữ các dữ liệu, thông tin như các trò chơi, các chương trình giải trí không lành mạnh, có nội dung xấu, không phục vụ công việc.

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

- Máy tính sử dụng để đọc, soạn thảo, lưu trữ, in ấn văn bản có nội dung là bí mật nhà nước.

- Máy tính xử lý thông tin trên hệ thống thông tin cấp độ 4 trở lên.

- Máy tính phục vụ quản trị hệ thống thông tin.

- Các máy chủ và thiết bị CNTT khác 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...).

- Các máy tính không bảo đảm an ninh, an toàn thông tin khi tham gia mạng máy tính của Bộ như: hệ điều hành không có bản quyền; không cài đặt chương trình diệt virus; thay đổi các thông số mạng của máy mà không thông báo và được sự đồng ý của Cục Công nghệ thông tin; cài đặt các phần mềm ứng dụng không bản quyền, không phục vụ mục đích công việc...

8. Chỉ cài đặt phần mềm hợp lệ và thuộc danh mục phần mềm được phép sử dụng trên máy tính được đơn vị cấp cho mình; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm khi chưa có sự đồng ý của bộ

phận chuyên trách về công nghệ thông tin; thường xuyên cập nhật phần mềm và hệ điều hành.

9. Cài đặt phần mềm phòng chống virus và thiết lập chế độ tự động cập nhật cho phần mềm, các đơn vị sử dụng mạng nội bộ của Bộ phải cài đặt chương trình phòng chống virus tập trung của Bộ; khi phát hiện bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy tính phải tắt máy và báo trực tiếp cho bộ phận chuyên trách về công nghệ thông tin để được xử lý kịp thời.

10. Chỉ truy nhập vào các trang/cổng thông tin điện tử, ứng dụng trực tuyến tin cậy và các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình.

**Điều 9. Quản lý tài khoản truy cập**

1. Tài khoản người dùng:

a) Đơn vị quản lý người dùng có văn bản đề nghị cấp tài khoản và phân quyền truy cập vào từng hệ thống thông tin, phần mềm ứng dụng cho người dùng của đơn vị mình.

Mỗi người dùng khi sử dụng hệ thống thông tin, phần mềm ứng dụng 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, có trách nhiệm bảo mật tài khoản truy nhập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác.

b) Trường hợp người dùng thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ hưu thì đơn vị quản lý người dùng phải thông báo bằng văn bản cho chủ quản hệ thống thông tin, phần mềm ứng dụng để thực hiện điều chỉnh, thu hồi, hủy bỏ các quyền sử dụng của người. Quy định cụ thể như sau:

- Văn bản đề nghị cấp mới/ thêm quyền/sửa quyền/ xóa tài khoản khi người dùng thay đổi vị trí công tác, chuyển công tác, thôi việc, nghỉ hưu phải gửi về chủ quản hệ thống thông tin, phần mềm ứng dụng. 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 chủ quản hệ thống thông tin, phần mềm ứng dụng bằng công văn hoặc theo cách thức quy định trong quy trình quản lý tài khoản CNTT áp dụng tại đơn vị chủ quản hệ thống thông tin, phần mềm ứng dụng.

- Tài khoản 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 Bộ, thôi việc, nghỉ hưu; không quá 05 ngày làm việc trong trường hợp thay đổi vị trí công tác hoặc chuyển công tác tới đơn vị khác thuộc Bộ.

- 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.

2. Tài khoản quản trị hệ thống:

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

b) Trường hợp cần thiết để bảo đảm an toàn, an ninh cho hệ thống, phải triển khai hệ thống quản lý tài khoản đặc quyền để thực hiện quản lý, lưu giữ, cấp phát tài khoản quản trị hệ thống.

3. Xác thực tài khoản:

a) Mật khẩu tài khoản dùng để truy cập hoặc sử dụng hoặc 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 (' ~ ! @ # $ % ^ & * () _ - + = { } [ ] \ I : ; “ ‘ <> , . ? /) 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 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.

4. Khi có yêu cầu khóa quyền truy cập hệ thống thông tin của tài khoản đang hoạt động, lãnh đạo đơn vị đang quản lý người dùng có tài khoản cần khóa phải yêu cầu bằng văn bản gửi đơn vị chủ quản hệ thống thông tin. Đơn vị vận hành hệ thống thông tin thực hiện việc khóa quyền truy cập của tài khoản khi có chỉ đạo của đơn vị chủ quản hệ thống thông tin. Đơn vị chủ quản hệ thống thông tin có quyền khóa quyền truy cập của tài khoản trong trường hợp tài khoản đó thực hiện các hành vi tấn công hoặc để xảy ra vấn đề mất an toàn, an ninh thông tin.

5. Hệ thống tài khoản CNTT phải được rà soát hàng năm, bảo đảm 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).

**Điều 10. Quản lý an toàn, an ninh thông tin mức ứng dụng**

1. Yêu cầu về bảo đảm an toàn thông tin phải được đưa vào tất cả các công đoạn thiết kế, xây dựng, triển khai và vận hành, sử dụng phần mềm, ứng dụng.

2. Phần mềm, ứng dụng phải đáp ứng các yêu cầu sau: cấu hình phần mềm, ứng dụng để xác thực người dùng; giới hạn số lần đăng nhập sai liên tiếp; giới hạn thời gian để chờ đóng phiên kết nối; mã hóa thông tin xác thực trên hệ thống; không để chế độ đăng nhập tự động...

3. Thiết lập, phân quyền truy nhập, quản trị, sử dụng tài nguyên khác nhau của phần mềm, ứng dụng với người dùng /nhóm người dùng có chức năng, yêu cầu nghiệp vụ khác nhau; tách biệt cổng giao tiếp quản trị phần mềm ứng dụng với cổng giao tiếp cung cấp dịch vụ; đóng các cổng giao tiếp không sử dụng.

4. Chỉ cho phép sử dụng các giao thức mạng có hỗ trợ chức năng mã hóa thông tin như SSH, SSL, VPN hoặc tương đương khi truy nhập, quản trị phần mềm, ứng dụng từ xa trên môi trường mạng; hạn chế truy cập đến mã nguồn của phần mềm, ứng dụng và phải đặt mã nguồn trong môi trường an toàn do bộ phận chuyên trách CNTT quản lý.

5. Các hệ thống thông tin bắt buộc phải có chức năng ghi và lưu trữ nhật ký về hoạt động của hệ thống và người dùng hệ thống thông tin. Ghi và lưu giữ bản ghi nhật ký hệ thống của phần mềm, ứng dụng trong khoảng thời gian tối thiểu 03 tháng với những thông tin cơ bản: thời gian, địa chỉ, tài khoản (nếu có), nội dung truy nhập và sử dụng phần mềm, ứng dụng; các lỗi phát sinh trong quá trình hoạt động; thông tin đăng nhập khi quản trị. Thực hiện việc bảo vệ các chức năng ghi nhật ký và thông tin nhật ký, chống giả mạo, sửa đổi, phá hủy và truy cập trái phép.

6. Chủ quản hệ thống thông tin tổ chức thực hiện kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin trong phạm vi cơ quan, tổ chức theo quy định tại Điều 20 Nghị định 85/2016/NĐ-CP.

Hệ thống thông tin và phần mềm ứng dụng phải được kiểm tra, đánh giá an toàn thông tin, đánh giá rủi ro an toàn thông tin và khắc phục các lỗ hổng bảo mật trước khi đưa vào sử dụng và trong quá trình sử dụng.

7. Thực hiện quy trình kiểm soát cài đặt, cập nhật, vá lỗi bảo mật phần mềm, ứng dụng trên các máy chủ, máy tính cá nhân, thiết bị kết nối mạng đang hoạt động thuộc hệ thống mạng nội bộ.

**Điều 11. Quản lý an toàn, an ninh thông tin mức dữ liệu**

1. Đơn vị phải thực hiện bảo vệ thông tin, dữ liệu liên quan đến hoạt động công vụ, thông tin có nội dung quan trọng, nhạy cảm hoặc không phải là thông tin công khai bằng các biện pháp như: thiết lập phương án bảo đảm tính bí mật, nguyên vẹn và khả dụng của thông tin, dữ liệu; mã hóa thông tin, dữ liệu khi lưu trữ trên hệ thống/thiết bị lưu trữ dữ liệu di động; sử dụng chữ ký số để xác thực và bảo mật thông tin, dữ liệu; xây dựng quy trình quản lý và phân công cán bộ quản lý.

2. Chủ quản hệ thống thông tin hoặc đơn vị được ủy quyền quản lý trực tiếp hệ thống thông tin triển khai hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng; phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau; thực hiện sao lưu dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

3. Không soạn thảo, lưu giữ tài liệu, vật chứa bí mật nhà nước trên máy tính, các thiết bị khác đã kết nối hoặc đang kết nối với mạng Internet, mạng máy tính, mạng viễn thông, trừ trường hợp lưu giữ bí mật nhà nước theo quy định của pháp luật về cơ yếu.

4. Các đơn vị thuộc Bộ phải thường xuyên kiểm tra, giám sát các hoạt động chia sẻ, gửi, nhận thông tin, dữ liệu trong hoạt động nội bộ của mình; khuyến cáo việc chia sẻ, gửi, nhận thông tin trên môi trường mạng cần phải sử dụng mật khẩu để bảo vệ thông tin.

5. Hoạt động sao chép và chuyển giao dữ liệu bảo mật ra khỏi hệ thống máy tính độc lập dùng để soạn thảo tài liệu mật phải tuân thủ theo đúng các quy định của Quy chế bảo vệ bí mật nhà nước.

6. Giao dịch trực tuyến phải được truyền đầy đủ, đúng địa chỉ, tránh bị sửa đổi, tiết lộ hoặc nhân bản một cách trái phép; sử dụng các cơ chế xác thực mạnh, chữ ký số khi tham gia giao dịch, sử dụng các giao thức truyền thông an toàn.

**Điều 12. Bảo đảm an toàn, an ninh thông tin trong việc quản lý cán bộ, công chức, viên chức và người lao động**

1. Phân công nhiệm vụ:

a) Xác định trách nhiệm trong việc bảo đảm an toàn thông tin mạng của vị trí phân công.

b) Bảo đảm người được phân công làm việc tại các vị trí có tiếp xúc với thông tin, dữ liệu bảo mật phải qua bước đánh giá, thẩm tra nhân thân và lý lịch.

c) Yêu cầu người được phân công phải cam kết bảo mật thông tin bằng văn bản riêng hoặc cam kết trong hợp đồng làm việc, hợp đồng lao động, bao gồm các điều khoản về trách nhiệm của cá nhân sau khi thôi việc tại đơn vị.

2. Sử dụng nguồn nhân lực:

Các đơn vị có trách nhiệm:

a) Sau khi tuyển dụng, tiếp nhận nhân sự mới, đơn vị phải có trách nhiệm phổ biến cho nhân sự mới các quy định về bảo đảm an toàn, an ninh thông tin tại đơn vị; đối với các vị trí tiếp xúc, quản lý các thông tin, dữ liệu quan trọng hoặc quản trị các hệ thống thông tin quan trọng, đơn vị phải yêu cầu nhân sự mới cam kết bảo mật thông tin bằng văn bản hoặc cam kết trong hợp đồng làm việc, hợp đồng lao động.

b) Có biện pháp quản lý tài khoản người dùng của cán bộ, công chức, viên chức và người lao động trên các hệ thống thông tin quan trọng.

c) Thường xuyên rà soát, kiểm tra quyền truy cập vào các hệ thống thông tin đối với tất cả cán bộ, công chức, viên chức và người lao động bảo đảm quyền truy cập phù hợp với nhiệm vụ được giao.

d) Phải thường xuyên tổ chức quán triệt các quy định về an toàn, an ninh thông tin, nhằm nâng cao nhận thức về trách nhiệm bảo đảm an toàn, an ninh thông tin của từng cá nhân trong đơn vị.

đ) Thực hiện đúng quy trình cấp mới, quản lý và thu hồi tài khoản, phân quyền truy cập các hệ thống thông tin và tất cả các tài sản liên quan đến hệ thống thông tin đối với các cá nhân do đơn vị quản lý.

3. Chấm dứt hoặc thay đổi công việc:

Khi cán bộ, công chức, viên chức và người lao động chấm dứt hoặc thay đổi công việc, cơ quan, đơn vị phải:

a) Xác định rõ trách nhiệm của cán bộ, công chức, viên chức, người lao động và các bên liên quan trong quản lý, sử dụng các tài sản CNTT được giao.

b) Lập biên bản bàn giao tài sản CNTT với đơn vị chủ quản và các đơn vị liên quan.

c) Thay đổi hoặc thu hồi quyền truy cập các hệ thống thông tin.

d) Rà soát, kiểm tra đối chiếu định kỳ giữa bộ phận quản lý nhân sự và bộ phận quản lý cấp phát, thu hồi quyền truy cập hệ thống thông tin để bảo đảm tài khoản người dùng của cán bộ, công chức, viên chức và người lao động đã nghỉ việc được thu hồi.

**Điều 13. Bảo đảm an toàn, an ninh thông tin khi tiếp nhận, phát triển, vận hành và bảo trì hệ thống thông tin**

1. 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 thông tin và thực hiện điều chỉnh, bổ sung hoặc thay mới hồ sơ đề xuất cấp độ trong trường hợp cần thiết.

2. Khi tiếp nhận, phát triển, nâng cấp, bảo trì hệ thống thông tin, đơn vị phải tiến hành phân tích, xác định rủi ro có thể xảy ra, đánh giá phạm vi tác động và phải chuẩn bị các biện pháp hạn chế, loại trừ các rủi ro này và yêu cầu các bên cung cấp, thi công, các cá nhân liên quan thực hiện.

3. Các hệ thống thông tin được cài đặt tại Trung tâm dữ liệu điện tử của Bộ Tư pháp cần đáp ứng các yêu cầu:

a) Tách biệt với các môi trường phát triển, kiểm tra và thử nghiệm;

b) Áp dụng các giải pháp bảo đảm an toàn thông tin;

c) Không cài đặt các công cụ, phương tiện phát triển ứng dụng;

d) Loại bỏ hoặc tắt các tính năng, phần mềm tiện ích không sử dụng trên hệ thống thông tin;

đ) Áp dụng các biện pháp bảo đảm tính toàn vẹn dữ liệu;

e) Mọi thao tác trên hệ thống phải được lưu vết, sẵn sàng cho kiểm tra, kiểm soát khi cần thiết.

4. Trong quá trình vận hành hệ thống thông tin, đơn vị chủ quản hệ thống thông tin cần thực hiện đánh giá, phân loại hệ thống thông tin theo cấp độ; triển khai phương án bảo đảm an toàn hệ thống thông tin đáp ứng yêu cầu cơ bản trong tiêu chuẩn, quy chuẩn kỹ thuật về bảo đảm an toàn hệ thống thông tin theo cấp độ; thường xuyên kiểm tra, giám sát an toàn hệ thống thông tin; tuân thủ quy trình vận hành, quy trình xử lý sự cố đã xây dựng; ghi lại và lưu trữ đầy đủ thông tin nhật ký hệ thống để phục vụ quản lý, kiểm soát thông tin.

5. Các đơn vị thuộc Bộ liên quan đến việc phát triển phần mềm ứng dụng có trách nhiệm yêu cầu các đối tác (nếu có) thực hiện các công tác bảo đảm an toàn thông tin, tránh lộ, lọt mã nguồn và dữ liệu, tài liệu thiết kế, quản trị hệ thống mà đối tác đang xử lý ra bên ngoài.

**Điều 14. Giám sát an toàn, an ninh thông tin mạng**

1. Nguyên tắc, yêu cầu, nội dung, phương thức, hệ thống kỹ thuật phục vụ công tác giám sát thực hiện theo quy định tại 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.

2. Chủ quản hệ thống thông tin chỉ đạo việc giám sát đối với các hệ thống thông tin thuộc phạm vi quản lý, phối hợp với Cục Công nghệ thông tin và các đơn vị chức năng chuyên trách về an toàn an ninh thông tin giám sát theo quy định.

**Điều 15. Kiểm tra, đánh giá an toàn, an ninh thông tin**

1. Chủ quản hệ thống thông tin có thẩm quyền yêu cầu kiểm tra, đánh giá đối với các hệ thống thông tin thuộc thẩm quyền quản lý. Đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin có thẩm quyền yêu cầu kiểm tra, đánh giá đối với các hệ thống thông tin do đơn vị này phê duyệt hồ sơ đề xuất cấp độ.

2. Đơn vị chủ trì kiểm tra, đánh giá là đơn vị được cấp có thẩm quyền giao nhiệm vụ hoặc được lựa chọn để thực hiện việc kiểm tra, đánh giá. Đối tượng kiểm tra, đánh giá là chủ quản hệ thống thông tin hoặc đơn vị vận hành hệ thống thông tin và các hệ thống thông tin có liên quan.

3. Nội dung, hình thức kiểm tra, đánh giá theo quy định tại Điều 11, Điều 12 Thông tư số 12/2022/TT-BTTTT.

4. Cục Công nghệ thông tin thực hiện việc đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin theo thẩm quyền. Nội dung đánh giá là cơ sở để điều chỉnh phương án bảo đảm an toàn thông tin cho phù hợp.

**Điều 16. Ứng cứu sự cố an toàn, an ninh thông tin mạng**

1. Đơn vị chuyên trách ứng cứu khẩn cấp sự cố an toàn thông tin mạng, Đội ứng cứu sự cố an toàn thông tin mạng Bộ Tư pháp

a) Cục Công nghệ thông tin là đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng của Bộ Tư pháp. 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.

b) Đội ứng cứu sự cố an toàn thông tin mạng Bộ Tư pháp (Đội ứng cứu sự cố) được thành lập theo quyết định 1246/QĐ-BTP ngày 30/5/2022 và tổ chức thực hiện ứng cứu, khắc phục sự cố an toàn thông tin mạng tại Bộ Tư Pháp. Quy chế hoạt động của Đội ứng cứu được ban hành theo Quyết định số 2216/QĐ-BTP ngày 11/11/2022 ban hành quy chế hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng Bộ Tư pháp.

2. Kế hoạch ứng phó sự cố bảo đảm an toàn, an ninh thông tin mạng

a) Các đơn vị thuộc Bộ 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 Công nghệ thông tin, báo cáo Bộ xem xét, quyết định.

b) Các kế hoạch ứng phó sự cố sau khi được phê duyệt phải gửi Cục Công nghệ thông tin tổng hợp thành kế hoạch chung của Bộ. Cục Công nghệ thông tin có trách nhiệm xây dựng kế hoạch ứng phó sự cố của Bộ, trình Lãnh đạo Bộ phê duyệt.

c) 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, an ninh thông tin năm tiếp theo.

3. Quy trình ứng cứu sự cố an toàn thông tin mạng

a) Các tổ chức, cá nhân khi phát hiện dấu hiệu tấn công hoặc sự cố an toàn thông tin mạng cần nhanh chóng báo cho đơn vị vận hành hệ thống thông tin, đơn vị chủ quản hệ thống thông tin liên quan, Cục

Công nghệ thông tin, Đội ứng cứu sự cố. Đội ứng cứu sự cố có trách nhiệm cập nhật, công khai thông tin liên lạc, đường dây nóng trên Cổng thông tin điện tử của Bộ.

b) 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 số 20/2017/TT-BTTT 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 (sau đây gọi tắt là Thông tư số 20/2017/TT-BTTT), đồng thời báo cáo Cục Công nghệ thông tin để tổng hợp, báo cáo lãnh đạo Bộ. Trách nhiệm của các đơn vị khi phát hiện, tiếp nhận xác minh, xử lý ban đầu và phân loại sự cố an toàn thông tin mạng theo quy định tại Điều 12 Quyết định 05/2017/QĐ-TTg và Điều 10 Thông tư số 20/2017/TT-BTTTT.

c) Quy trình ứng cứu sự cố an toàn thông tin mạng theo quy định tại Điều 13, Điều 14 Quyết định 05/2017/QĐ-TTg và Điều 11 Thông tư số 20/2017/TT-BTTTT.

4. Diễn tập ứng cứu sự cố an toàn thông tin mạng

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 Công nghệ thông tin và Đội ứng cứu sự cố 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 hàng năm trong phạm vi Bộ Tư pháp.

**Điều 17. Phong tỏa, hạn chế hoạt động của hệ thống thông tin**

1. Việc áp dụng biện pháp phong tỏa, hạn chế hoạt động của hệ thống thông tin được tiến hành trong trường hợp khi có căn cứ hệ thống thông tin đã mất an toàn, an ninh thông tin hoặc bị lợi dụng không gian mạng để khủng bố hoặc thực hiện hành vi vi phạm pháp luật.

2. Trình tự thủ tục thực hiện:

a) Cục Công nghệ thông tin phối hợp với chủ quản hệ thống thông tin khẩn cấp thực hiện biện pháp phong tỏa, hạn chế hoạt động của hệ thống thông tin.

b) Cục Công nghệ thông tin phối hợp với chủ quản hệ thống thông tin báo cáo Lãnh đạo Bộ. Đồng thời, thực hiện thông báo và phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thực hiện theo trình tự, thủ tục quy định tại Nghị định 04/2019/NĐ-CP ngày 27/12/2019 và Nghị định 101/2016/NĐ-CP ngày 01/7/2016.

## Chương III

## TRÁCH NHIỆM CỦA CÁC TỔ CHỨC, CÁ NHÂN

**Điều 18. Trách nhiệm của Cục Công nghệ thông tin**

1. Thực hiện trách nhiệm của đơn vị chuyên trách về an toàn thông tin theo quy định tại Điều 21 Nghị định 85/2016/NĐ-CP và Quy chế này.

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

3. Xây dựng kế hoạch, báo cáo về an toàn, an ninh thông tin mạng của Bộ Tư pháp.

4. Bảo đảm an toàn, an ninh thông tin cho các hệ thống thông tin, cơ sở dữ liệu dùng chung của Bộ.

5. Đôn đốc, giám sát, kiểm tra và báo cáo Bộ việc thực hiện Quy chế này tại các đơn vị thuộc Bộ.

6. Xây dựng kế hoạch tuyên truyền, phổ biến nâng cao nhận thức về an toàn, an ninh thông tin mạng tại Bộ Tư pháp và thực hiện các nội dung theo kế hoạch đã được phê duyệt.

7. Cục Công nghệ thông tin phối hợp với Vụ Tổ chức cán bộ xây dựng, trình Bộ trưởng phê duyệt kế hoạch dài hạn, kế hoạch hàng năm về đào tạo, bồi dưỡng nghiệp vụ an toàn, an ninh thông tin cho cán bộ, công chức, viên chức và người lao động của Bộ và tổ chức đào tạo theo kế hoạch đã phê duyệt.

**Điều 19. Trách nhiệm của Vụ Tổ chức Cán bộ**

Căn cứ nhu cầu về đào tạo nguồn nhân lực bảo đảm an toàn thông tin của các đơn vị thuộc Bộ, phối hợp với Cục Công nghệ thông tin xây dựng trình Bộ phê duyệt kế hoạch dài hạn, kế hoạch hàng năm về đào tạo, bồi dưỡng nghiệp vụ an toàn, an ninh thông tin cho cán bộ, công chức, viên chức và người lao động của Bộ và thực hiện tổ chức đào tạo theo kế hoạch đã phê duyệt.

**Điều 20. Trách nhiệm của các đơn vị thuộc Bộ**

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

2. Thực hiện các báo cáo theo quy định, gửi Cục Công nghệ thông tin tổng hợp, báo cáo Bộ.

3. Triển khai quy chế bảo đảm an toàn, an ninh thông tin tại đơn vị bảo đảm phù hợp với Quy chế này và các yêu cầu cụ thể của đơn vị.

4. Thực hiện việc quản lý trang thiết bị CNTT và cán bộ, công chức, viên chức, người lao động theo Quy chế này.

5. Phối hợp với Cục Công nghệ thông tin bảo đảm an toàn, an ninh thông tin cho các hệ thống thông tin, cơ sở dữ liệu dùng chung của Bộ và các hệ thống thông tin do đơn vị quản lý, vận hành.

6. Thường xuyên kiểm tra, theo dõi và đánh giá công tác bảo đảm an toàn, an ninh thông tin mạng tại cơ quan, đơn vị mình, coi đây là nhiệm vụ trọng tâm của đơn vị.

8. Thường xuyên tổ chức các hoạt động tuyên truyền, phổ biến nâng cao nhận thức về bảo đảm an toàn, an ninh thông tin đến toàn thể cán bộ, công chức, viên chức và người lao động tại đơn vị.

**Điều 21. Trách nhiệm của chủ quản hệ thống thông tin**

1. Thực hiện trách nhiệm của đơn vị chủ quản hệ thống thông tin theo quy định tại Điều 20 Nghị định 85/2016/NĐ-CP và Quy chế này.

2. Chỉ đạo, phân công các đơn vị vận hành các hệ thống thông tin triển khai công tác bảo đảm an toàn thông tin trong tất cả các công đoạn liên quan đến hệ thống thông tin.

**Điều 22. Trách nhiệm của đơn vị vận hành hệ thống thông tin**

1. Thực hiện trách nhiệm của đơn vị vận hành hệ thống thông tin theo quy định tại Điều 22 Nghị định số 85/2016/NĐ-CP và các nhiệm vụ do chủ quản hệ thống thông tin phân công.

2. 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.

**Điều 23. Trách nhiệm cá nhân**

1. Thủ trưởng đơn vị thuộc Bộ có trách nhiệm: phổ biến tới từng cán bộ, công chức, viên chức, người lao động của đơn vị; tổ chức triển khai và thường xuyên kiểm tra việc thực hiện Quy chế này tại đơn vị; chịu trách nhiệm trước pháp luật và Lãnh đạo Bộ Tư pháp về các vi phạm, thất thoát thông tin, dữ liệu bảo 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 của Bộ Tư pháp, 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 bảo mật của ngành Tư pháp do vi phạm Quy chế; tự cập nhật kiến thức về an ninh mạng và an toàn thông tin đã được đưa lên trang thông tin của Cục Công nghệ thông tin.

## Chương IV

## TỔ CHỨC THỰC HIỆN

### Điều 24. Nguồn lực thực hiện

1. Kinh phí bảo đảm an toàn, an ninh thông tin mạng theo cấp độ từ nguồn vốn ngân sách nhà nước và các nguồn vốn hợp pháp theo quy định của pháp luật.

2. Kinh phí đầu tư cho bảo đảm an toàn, an ninh thông tin mạng sử dụng vốn ngân sách nhà nước. Đối với dự án đầu tư công để xây dựng mới hoặc mở rộng, nâng cấp hệ thống thông tin, kinh phí đầu tư cho bảo đảm an toàn, an ninh thông tin mạng theo cấp độ được bố trí trong vốn đầu tư của dự án tương ứng.

3. Kinh phí thực hiện giám sát, quản lý rủi ro an toàn, an ninh thông tin mạng; đào tạo ngắn hạn, tuyên truyền, phổ biến nâng cao nhận thức, diễn tập an toàn thông tin và ứng cứu sự cố được lập và bố trí trong dự toán chi thường xuyên hàng năm của Bộ theo quy định của Pháp luật.

4. Căn cứ nhiệm vụ được giao, các cơ quan, tổ chức thuộc Bộ thực hiện lập dự toán, sử dụng và quyết toán kinh phí thực hiện nhiệm vụ bảo đảm an toàn thông tin theo quy định của Luật Ngân sách Nhà nước.

### Điều 25. Khen thưởng, kỷ luật

1. Kết quả thực hiện Quy chế này là một trong những tiêu chí đánh giá kết quả thực hiện hàng năm của cá nhân, đơn vị đồng thời là tiêu chí bắt buộc để xem xét tình hình khen thưởng và danh hiệu thi đua đối với các tổ chức, cá nhân.

2. Đơn vị, cá nhân vi phạm Quy chế này và các quy định khác của pháp luật về bảo đảm an toàn, an ninh thông tin mạng, tùy theo tính chất, mức độ vi phạm sẽ bị xử lý kỷ luật hoặc các hình thức xử lý khác theo quy định của pháp luật; nếu vi phạm gây thiệt hại đến tài sản, thông tin, dữ liệu thì chịu trách nhiệm bồi thường theo pháp luật hiện hành.

### Điều 26. Tổ chức thực hiện

1. Thủ trưởng các đơn vị thuộc Bộ phổ biến, quán triệt và tổ chức thực hiện Quy chế này trong phạm vi đơn vị.

2. Cục Công nghệ thông tin theo dõi, đôn đốc, kiểm tra các đơn vị thực hiện Quy chế này; hàng năm kiểm tra, tổng kết, đánh giá và báo cáo trình Bộ trưởng.

3. Tổng cục Thi hành án dân sự thực hiện xây dựng Quy chế bảo đảm an toàn, an ninh thông tin mạng cho Hệ thống các cơ quan Thi hành án dân sự.

4. Vụ Tổ chức cán bộ chủ trì, phối hợp với Cục Công nghệ thông tin trong việc đào tạo, bồi dưỡng nghiệp vụ an toàn, an ninh thông tin cho cán bộ, công chức, viên chức và người lao động của Bộ.

5. Trường hợp các văn bản quy phạm pháp luật được dẫn chiếu tại Quy chế này được bãi bỏ, thay thế, sửa đổi, bổ sung thì thực hiện theo văn bản quy phạm pháp luật mới.

6. Trong quá trình tổ chức thực hiện, nếu có những vấn đề vướng mắc các đơn vị kịp thời phản ánh về Cục Công nghệ thông tin để tổng hợp, trình Bộ trưởng xem xét, quyết định việc sửa đổi, bổ sung cho phù hợp với tình hình thực tế và các quy định của pháp luật./.