| BỘ TƯ PHÁP | CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM |
|---|---|
| | Độc lập - Tự do - Hạnh phúc |

# QUY CHẾ

**Quản lý, vận hành, khai thác, sử dụng và đảm bảo an toàn thông tin hệ thống mạng máy tính của Bộ Tư pháp**

(*Ban hành kèm theo Quyết định số 299/QĐ-BTP ngày 08 tháng 02 năm 2014 của Bộ trưởng Bộ Tư pháp*)

## Chương I

## NHỮNG QUY ĐỊNH CHUNG

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

Quy chế này quy định về việc quản lý, vận hành, khai thác, sử dụng và đảm bảo an toàn thông tin hệ thống mạng máy tính của Bộ Tư pháp.

Quy chế này được áp dụng đối với các đơn vị, cán bộ, công chức, viên chức và người lao động của các đơn vị thuộc Bộ Tư pháp (sau đây gọi là các đơn vị và cá nhân) và cơ quan, tổ chức, cá nhân có liên quan trong việc quản lý, vận hành, khai thác, sử dụng và bảo vệ hệ thống mạng máy tính của Bộ Tư pháp.

### Điều 2. Hệ thống mạng máy tính của Bộ Tư pháp

Hệ thống mạng máy tính của Bộ Tư pháp là mạng riêng, bao gồm: mạng nội bộ tại Bộ Tư pháp, mạng riêng ảo và mạng nội bộ tại các đơn vị.

Trung tâm hệ thống mạng máy tính đặt tại Trung tâm dữ liệu điện tử của Bộ Tư pháp do Cục Công nghệ thông tin quản lý.

Hệ thống mạng máy tính của Bộ Tư pháp được sử dụng để phục vụ cho công tác quản lý, chỉ đạo, điều hành, các công tác chuyên môn nghiệp vụ, phối hợp công tác trong ngành Tư pháp.

### Điều 3. Giải thích thuật ngữ

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

1. Mạng nội bộ (LAN - Local Area Network): là một hệ thống mạng bao gồm các máy tính và các thiết bị ngoại vi được liên kết với nhau. Người sử

dụng mạng nội bộ có thể chia sẻ tài nguyên như thông tin, dữ liệu, các phần mềm dùng chung, các ứng dụng chuyên ngành, các công cụ tiện ích và các thiết bị ngoại vi.

2. Cơ sở dữ liệu (Database): là một hệ thống các thông tin có cấu trúc được lưu trữ trên các thiết bị lưu trữ thông tin thứ cấp (như băng từ, đĩa từ...) để có thể thỏa mãn yêu cầu khai thác thông tin đồng thời của nhiều người sử dụng hay nhiều chương trình ứng dụng với nhiều mục đích khác nhau.

3. Tài khoản (Account): là đại diện cho đơn vị, cá nhân trên mạng, bao gồm tên tài khoản và mật khẩu dùng để truy cập. Sau khi đã đăng nhập vào mạng, cá nhân có quyền khai thác và sử dụng các tài nguyên của mạng tuỳ thuộc vào quyền truy cập được cấp cho tài khoản cho đến khi rời khỏi mạng. Cơ sở dữ liệu tài khoản được tổ chức, quản lý bởi quản trị hệ thống.

4. Thông số mạng: là các tập hợp các tham số kỹ thuật do Cục Công nghệ thông tin thiết lập nhằm đảm bảo sự thống nhất trong việc sử dụng và quản lý các tài nguyên trên hệ thống mạng máy tính của Bộ Tư pháp.

5. Mạng riêng ảo của Bộ Tư pháp (VPN - Virtual Private Network) : là một mạng dành riêng để kết nối các máy tính bên ngoài trụ sở Bộ vào mạng nội bộ thông qua Internet. Với VPN, tất cả kết nối giữa các máy tính đều được mã hóa và có độ an toàn cao, cá nhân có thể thiết lập kết nối từ xa để sử dụng các dịch vụ, ứng dụng như đang trong mạng nội bộ của Bộ Tư Pháp.

6. "Đảm bảo an toàn thông tin" là đảm bảo tính bí mật, tính toàn vẹn, tính chống chối bỏ và tính sẵn sàng của thông tin, trong đó:

- Tính bí mật: Bảo đảm thông tin chỉ có thể được truy cập bởi những người có thẩm quyền đối với thông tin.

- Tính toàn vẹn: thông tin không bị sửa đổi làm sai lệch nội dung.

- Tính chống chối bỏ: các cá nhân tham gia vào hệ thống mạng, sử dụng các ứng dụng của Bộ Tư pháp không thể chối bỏ các hoạt động đã thực hiện. Tính chống chối bỏ cung cấp các bằng chứng chống lại việc chối bỏ một hành động đã thực hiện hay đã diễn ra.

- Tính sẵn sàng: Bảo đảm những người được cấp quyền có thể truy cập sử dụng thông tin ngay khi có nhu cầu.

7. Virus: virus là một loại đoạn chương trình, mã độc hại có khả năng tự nhân bản và lây nhiễm chính nó vào các file, chương trình hoặc máy tính.

8. “Mật khẩu phức tạp”: là mật khẩu đáp ứng yêu cầu sau:

- Có tối thiểu 8 ký tự.

- Gồm tối thiểu 3 trong số 4 loại ký tự sau: chữ cái viết hoa (A-Z), chữ cái viết thường (a-z), chữ số (0-9), các ký tự đặc biệt trên bàn phím máy tính (~, !, @ …)

## Chương II
## QUẢN LÝ, VẬN HÀNH, KHAI THÁC, SỬ DỤNG HỆ THỐNG MẠNG MÁY TÍNH CỦA BỘ TƯ PHÁP

### Điều 4. Trách nhiệm quản lý và vận hành hệ thống mạng máy tính của Bộ Tư pháp

1. Cục Công nghệ thông tin Bộ Tư pháp giúp Bộ trưởng thực hiện nhiệm vụ quản lý và vận hành hệ thống mạng máy tính của Bộ Tư pháp có trách nhiệm sau:

a. Quản lý vận hành và hỗ trợ kỹ thuật cho các đơn vị và cá nhân khai thác tài nguyên trên hệ thống mạng máy tính của Bộ Tư pháp có hiệu quả và đảm bảo an toàn thông tin.

b. Quản lý hệ thống mạng máy tính theo tiêu chuẩn kỹ thuật về dữ liệu và thiết lập thông số mạng phù hợp với các quy định của cơ quan có thẩm quyền ban hành về hệ thống mạng máy tính.

2. Các đơn vị thuộc Bộ, tổ chức và cá nhân có liên quan có trách nhiệm quản lý các trang thiết bị, dữ liệu trên máy tính của đơn vị, cá nhân và khai thác, sử dụng thông tin trên hệ thống mạng máy tính của Bộ Tư pháp phục vụ yêu cầu công tác theo các quy định tại quy chế này.

### Điều 5. Khai thác, sử dụng hệ thống mạng máy tính của Bộ Tư pháp

1. Cục Công nghệ thông tin áp dụng các biện pháp cần thiết để đảm bảo hoạt động kết nối Internet của cá nhân tại đơn vị được an toàn và thông suốt.

2. Các đơn vị khi có nhu cầu kết nối vào hệ thống mạng máy tính của Bộ Tư pháp 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 khác tham gia vào hệ thống mạng nội bộ.

4. Các cơ quan bên ngoài khi có kết nối trực tiếp vào mạng nội bộ của Bộ Tư pháp phải được sự đồng ý của Bộ Tư pháp 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 người dùng để truy cập vào hệ thống mạng máy tính của Bộ Tư pháp; khi đã đăng nhập vào mạng cá nhân có quyền khai thác cơ sở dữ liệu và sử dụng các tài nguyên của mạng theo quy định của Bộ.

6. Các cá nhân không được sử dụng hệ thống mạng máy tính của Bộ Tư pháp 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. Các cá nhân không tự ý sử dụng các trang thiết bị mạng và viễn thông để kết nối vào hệ thống mạng Bộ Tư pháp.

**Điều 6. Phần mềm, ứng dụng trong hệ thống mạng máy tính Bộ Tư pháp**

1. Các phần mềm, ứng dụng khi vận hành trong hệ thống mạng máy tính của Bộ Tư pháp tối thiểu phải đáp ứng những yêu cầu sau:

a. Phải được kiểm tra, thử nghiệm đáp ứng tiêu chuẩn an toàn thông tin trước khi đưa vào sử dụng trong hệ thống mạng máy tính của Bộ Tư pháp.

b. Việc sử dụng, trang bị phần mềm hệ thống, phần mềm tiện ích và ứng dụng công nghệ thông tin phải tuân thủ theo Luật bản quyền.

c. Đảm bảo tính toàn vẹn của dữ liệu khi lưu chuyển trong hệ thống mạng Bộ Tư pháp.

2. Cục Công nghệ thông tin có trách nhiệm xây dựng quy trình hoạt động, thử nghiệm, trực tiếp cài đặt, quản lý và vận hành phần mềm hệ thống, phần mềm tiện ích và ứng dụng công nghệ thông tin trong hệ thống mạng máy tính của Bộ Tư pháp; nghiên cứu, đề xuất, nâng cấp công nghệ phần mềm theo định hướng quản lý nhà nước của ngành Tư pháp và tuân theo quy định của pháp luật.

Thực hiện kiểm tra thường xuyên nhằm phát hiện và khắc phục lỗ hổng bảo mật của phần mềm, ứng dụng; cập nhật các bản nâng cấp mới và các bản vá lỗi cho phần mềm hệ thống.

3. Các đơn vị và cá nhân không được tự ý cài đặt các phần mềm, ứng dụng vào hệ thống mạng máy tính của Bộ Tư pháp, không được tự ý làm thay đổi các thông số của các thiết bị trong hệ thống mạng máy tính. Trong trường hợp các đơn vị, cá nhân có nhu cầu cài đặt mới, thay đổi, gỡ bỏ,.. các phần mềm, ứng dụng để phục vụ hoạt động chuyên môn của đơn vị thì phải phối hợp cho Cục Công nghệ thông tin để thực hiện nhằm đảm bảo an toàn thông tin chung.

**Điều 7. Quản trị hệ thống mạng**

Cục Công nghệ thông tin khi thực hiện nhiệm vụ quản trị hệ thống mạng máy tính của Bộ Tư pháp có trách nhiệm sau:

1. Quản lý, vận hành, nâng cấp, bảo trì, sửa chữa và giám sát hệ thống mạng máy tính của Bộ; phát hiện các hành vi sử dụng mạng không hợp lệ; xử lý các lỗi kỹ thuật; ngăn ngừa các sự cố trên mạng để đảm bảo tính an toàn, tính tin cậy và đảm bảo sự vận hành thông suốt hệ thống mạng máy tính của Bộ Tư pháp.

2. Thực hiện việc sao lưu dữ liệu theo kế hoạch.

3. Ghi nhật ký ca trực và thực hiện báo cáo định kỳ hoặc đột xuất khi có sự cố cho Thủ trưởng đơn vị để phối hợp xử lý.

4. Cấp địa chỉ mạng (IP address) và thông số mạng cho các đơn vị và cá nhân tham gia hệ thống mạng máy tính của Bộ Tư pháp.

5. Lọc bỏ, chặn truy cập hoặc hạn chế truy cập các trang tin, ứng dụng có nghi ngờ chứa mã độc hoặc các nội dung không phù hợp phục vụ công việc.

6. Thông báo, tạm ngừng cung cấp dịch vụ; trong trường hợp nghiêm trọng có thể thu hồi tài nguyên mạng và báo cáo các cấp có thẩm quyền để xử lý đối với các đơn vị và cá nhân vi phạm các nguyên tắc quản lý và khai thác tài nguyên hệ thống mạng máy tính của Bộ Tư pháp.

7. Đào tạo cán bộ quản lý, triển khai, vận hành hệ thống công nghệ thông tin có kiến thức chuyên môn, nghiệp vụ về công nghệ thông tin đáp ứng yêu cầu.

8. Phối hợp với các đơn vị có thẩm quyền như : Bộ Công an, Ban Cơ yếu chính phủ, Trung tâm ứng cứu khẩn cấp máy tính Việt Nam (VN-CERT) và các đơn vị khác có liên quan để thường xuyên theo dõi và phối hợp ngăn ngừa nguy cơ tấn công mạng đảm bảo an toàn thông tin.

9. Có biện pháp dự phòng về thiết bị, phần mềm đối với các hệ thống mạng và ứng dụng, để đảm bảo sự hoạt động liên tục của hệ thống.

10. Cần cập nhật bản vá hệ điều hành, mẫu phòng diệt virus, các mẫu lỗ hổng bảo mật, mẫu tấn công,... đối với máy chủ và thiết bị tin học, chỉ thiết lập kết nối Internet cho các máy chủ hoặc thiết bị cần phải có giao tiếp ra Internet (các máy chủ, thiết bị cung cấp giao diện ra Internet như trang Cổng thông tin điện tử, các dịch vụ công, thư điện tử…).

**Điều 8. Quản lý, sử dụng thiết bị tin học**

1. Trang thiết bị tin học được trang bị tại các tòa nhà, đơn vị và các thiết bị tin học được trang bị cho cá nhân là tài sản Nhà nước, được quản lý, sử dụng theo quy định của pháp luật về quản lý tài sản Nhà nước.

2. Các đơn vị và cá nhân có trách nhiệm quản lý trang thiết bị tin học được giao, tự bảo quản dữ liệu trên máy. Trong quá trình sử dụng các trang thiết bị tin học, nếu có sự cố xảy ra, các đơn vị, cá nhân, có trách nhiệm phối hợp với Cục Công nghệ thông tin để tìm biện pháp khắc phục sự cố.

3. Các trang thiết bị tin học do các đơn vị tự mua sắm phải theo hướng dẫn của Cục Công nghệ thông tin để đảm bảo tiêu chuẩn kỹ thuật trong việc sử dụng và tham gia kết nối và khai thác hệ thống thông tin của Bộ.

4. Các đơn vị và cá nhân sử dụng thiết bị đã kết nối với hệ thống mạng máy tính của Bộ không được tự ý bỏ kết nối, thay đổi các thông số đã được cài đặt của các thiết bị.

## Chương III
## ĐẢM BẢO AN TOÀN THÔNG TIN

**Điều 9. Đảm bảo an toàn thiết bị**

1. Trung tâm dữ liệu điện tử bao gồm khu vực chứa máy chủ và thiết bị lưu trữ, các tủ mạng và đấu nối mạng tới các tòa nhà, thiết bị nguồn điện và dự phòng điện khẩn cấp, phòng vận hành, kiểm soát (quản trị) hệ thống phải được

kiểm soát truy cập vật lý để phòng tránh truy cập trái phép hoặc sai mục đích. Cục Công nghệ thông tin xây dựng nội quy hướng dẫn làm việc trong Trung tâm dữ liệu điện tử.

2. Các cá nhân 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 lưu thông tin có trách nhiệm bảo vệ các thiết bị này và thông tin lưu trên thiết bị, tránh làm mất, lộ thông tin; 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. Nghiêm cấm sử dụng thiết bị do cá nhân tự trang bị để lưu giữ bí mật Nhà nước.

3. Các thiết bị lưu trữ không sử dụng tiếp cho công việc của đơn vị (thanh lý, cho, tặng) phải được xóa nội dung bằng phần mềm hoặc bằng thiết bị hủy dữ liệu chuyên dụng hay phá hủy vật lý.

**Điều 10. Đảm bảo an toàn dữ liệu**

1. Phân loại thông tin: Tiến hành phân loại thông tin, dữ liệu theo mức độ quan trọng, giá trị của thông tin đối với cơ quan, đơn vị về tần xuất sử dụng, thời gian lưu trữ và giá trị pháp lý của nó, bảo đảm thông tin đó và tài sản gắn liền với các phương tiện xử lý thông tin một cách thích hợp cho việc phân loại.

2. Áp dụng các thuật toán mã hóa cho các hoạt động sau: đăng nhập quản trị hệ thống; đăng nhập vào các ứng dụng; gửi nhận dữ liệu tự động giữa các máy chủ; nhập và biên tập dữ liệu; tra cứu dữ liệu mật, quan trọng.

3. Các thông tin quan trọng phải được mã hóa bằng thuật toán mã hóa an toàn hoặc sử dụng công nghệ chữ ký số để xác thực và mã hóa bảo mật dữ liệu.

4. Nghiêm cấm việc soạn thảo, trao đổi, lưu trữ thông tin, tài liệu bí mật nhà nước trên máy tính có nối mạng Internet. Các cơ quan, đơn vị phải bố trí máy vi tính riêng, không kết nối mạng nội bộ và Internet dùng để soạn thảo văn bản, lưu giữ thông tin có nội dung mật theo quy định.

5. Cục Công nghệ thông tin xây dựng quy trình, nhân sự phục vụ công tác bảo quản, sao lưu dữ liệu và định kỳ kiểm tra dữ liệu đã sao lưu, việc sao lưu dữ liệu được thực hiện trên hệ thống sao lưu đặt tại Trung tâm dữ liệu điện tử của Bộ Tư pháp.

6. Các cá nhân được phân công thực hiện soạn thảo, gửi, nhận dữ liệu có trách nhiệm xác định mức độ mật, quan trọng của dữ liệu để thực hiện phương

thức bảo vệ dữ liệu phù hợp hoặc yêu cầu Cục Công nghệ thông tin hướng dẫn, hỗ trợ phương thức bảo vệ trong trường hợp cần thiết.

**Điều 11. Quản lý các tài khoản trong hệ thống**

1. Tài khoản cá nhân

a. Mỗi cá nhân khi sử dụng hệ thống mạng, các ứng dụng của Bộ Tư pháp được cấp tài khoản truy cập với định danh duy nhất gắn với cá nhân đó. Trường hợp tài khoản dùng chung cho một đơn vị hay một tổ chức thì lãnh đạo đơn vị, tổ chức có trách nhiệm quản lý hoặc ủy quyền cho một cá nhân quản lý tài khoản đó.

b. Thực hiện đổi mật khẩu định kỳ, tối thiểu 3 tháng một lần.

c. Mọi trường hợp cấp mới, cấp lại tài khoản và mật khẩu cho đơn vị, cá nhân phải có công văn đề nghị qua đường bưu điện hoặc gửi công văn qua thư điện tử có chữ ký số của lãnh đạo đơn vị. Khi đơn vị có cán bộ chuyển vị trí công tác hoặc nghỉ việc thì đơn vị phải có trách nhiệm thông báo cho Cục Công nghệ thông tin để tiến hành điều chỉnh, thu hồi, hủy bỏ các quyền truy cập hệ thống và các ứng dụng đối với cán bộ đó hoặc chuyển đổi tài khoản cá nhân cho phù hợp với vị trí mới nhằm tránh tình trạng truy cập không đúng thẩm quyền vào hệ thống.

d. Cục Công nghê thông tin phối hợp với các đơn vị định kỳ rà soát lại các quyền truy nhập đã cấp phát nhằm phát hiện ra tình trạng phân quyền gây mất an toàn như: vượt quyền, không thu hồi khi người sử dụng đã hết quyền sử dụng, quá thời hạn sử dụng,...

2. Tài khoản quản trị:

a. Tài khoản quản trị (thiết bị mạng, các ứng dụng, phần mềm hệ thống, cơ sở dữ liệu…) phải tách biệt với tài khoản truy cập mạng, ứng dụng với tư cách cá nhân thông thường.

b. Tài khoản quản trị phải có định danh duy nhất và gắn với trách nhiệm cá nhân. Nghiêm cấm dùng chung tài khoản quản trị.

c. Mật khẩu phức tạp phải được áp dụng cho tất cả các tài khoản truy cập, sử dụng, quản trị hệ thống mạng, các ứng dụng trên hệ thống mạng máy tính của Bộ Tư pháp.

d. Thực hiện đổi mật khẩu định kỳ, tối thiểu 2 tháng một lần.

đ. Cá nhân, 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.

**Điều 12. Đảm bảo an toàn trong công tác quản trị hệ thống**

1. Máy tính dùng để quản trị hệ thống chỉ được cài đặt các phần mềm cần thiết cho hoạt động quản trị hệ thống, đặt trong vùng mạng phục vụ công tác quản trị hệ thống và chỉ được cấp quyền truy cập cho các cá nhân được giao trách nhiệm quản trị hệ thống.

2. Thường xuyên được kiểm tra cài đặt các bản cập nhật mới cho các thiết bị tường lửa bên ngoài, tường lửa ứng dụng, IPS, Proxy, thiết bị chống Spam mail … để khắc phục các điểm yếu; Có chế độ bảo trì, bảo hành hoặc thiết bị dự phòng để đảm bảo sự hoạt động liên tục của hệ thống

3. Cá nhân làm công tác quản trị hệ thống phải thay đổi mật khẩu mặc định tài khoản quản trị của mình ngay khi được bàn giao.

4. Sử dụng kênh trao đổi thông tin an toàn (có mã hóa) khi truy cập quản trị hệ thống.

5. Tất cả các truy cập quản trị hệ thống đăng nhập (log-in), đăng xuất (log-out); các lần xác thực thành công hoặc thất bại; thời gian xảy ra; các hành động, thao tác thực thi các công cụ hệ thống,... khi quản trị viên của thực hiện đều phải được ghi nhật ký quản trị để phục vụ cho việc theo dõi và quản lý.

**Điều 13. Đảm bảo an toàn thông tin**

1. Đối với các đơn vị và cá nhân

a. Các đơn vị cử cán bộ tham gia các lớp tập huấn, bồi dưỡng do Cục Công nghệ thông tin tổ chức để trang bị các kiến thức về an toàn thông tin phù hợp trước khi cho phép truy cập, vận hành, khai thác và sử dụng hệ thống thông tin.

b. Cá nhân chỉ được sử dụng máy tính do lãnh đạo đơn vị giao cho, không được phép sử dụng máy tính của người khác khi chưa được lãnh đạo đơn vị đồng ý.

c. Cá nhân đặt chế độ bảo vệ màn hình và mật khẩu sử dụng máy tính để đảm bảo an toàn cho dữ liệu cá nhân, khi không làm việc với máy tính trong thời gian dài phải thoát khỏi phiên làm việc và tắt máy. Mật khẩu tài khoản của cá nhân yêu cầu đặt mật khẩu phức tạp với độ an toàn cao để truy cập mạng, không được chuyển cho người khác sử dụng.

d. Hạn chế việc sử dụng chức năng chia sẻ tài nguyên (sharing), khi sử dụng chức năng này cần bật thuộc tính bảo mật bằng mật khẩu khi chia sẻ dữ liệu, tránh chia sẻ trực tiếp với chế độ truy cập đọc/ghi và thực hiện việc thu hồi chức năng này khi đã sử dụng xong.

2. Đối với Cục Công nghệ thông tin:

a. Hàng năm có trách nhiệm tổ chức các lớp tập huấn, bồi dưỡng để trang bị kiến thức phù hợp về an toàn thông tin trước khi cho phép truy cập, vận hành, khai thác và sử dụng hệ thống thông tin.

b. Áp dụng các biện pháp đảm bảo an toàn, bảo mật những thông tin truyền dẫn trên hệ thống mạng máy tính của Bộ Tư pháp.

c. Bố trí cán bộ chuyên trách về an toàn hệ thống thông tin trên môi trường máy tính và hệ thống mạng máy tính (bao gồm công tác giám sát, kiểm tra việc thực hiện quy định này tại Bộ Tư pháp).

d. Ban hành quy trình cụ thể về việc phát hiện, báo cáo, xử lý và quản lý hoạt động khắc phục các sự cố liên quan đến an toàn thông tin tại Bộ Tư pháp.

đ. Giám sát thường xuyên các hệ thống an ninh mạng để đảm bảo tác dụng của hệ thống, đồng thời phát hiện và xử lý sớm các vấn đề về an toàn thông tin. Thực hiện kết xuất định kỳ hàng tháng hoặc hàng quý các báo cáo từ hệ thống an ninh mạng để theo dõi, đánh giá các vấn đề của hệ thống.

e. Thường xuyên nghiên cứu, cập nhật các kiến thức về an toàn thông tin, có biện pháp phòng tránh các nguy cơ tiềm ẩn có thể gây mất thông tin khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ.

f. Kịp thời thông báo cho các đơn vị, người sử dụng biết khi tạm dừng để nâng cấp, bảo trì định kỳ, khắc phục sự cố của từng dịch vụ mạng hoặc hệ thống mạng máy tính nội bộ.

**Điều 14. Phòng, chống virus tin học**

1. Cục Công nghệ thông tin có trách nhiệm:

a. Duy trì hệ thống phòng chống virus, giảm thiểu tối đa tác hại của việc lây lan, tấn công của các loại virus, các loại mã nguồn độc hại và ngăn chặn kịp thời sự bùng nổ virus trong mạng nội bộ.

b. Thường xuyên cập nhật, cung cấp các phiên bản mới, các bản vá lỗi của phần mềm chống virus để bảo đảm chương trình quét virus của các đơn vị và cá nhân trên các máy chủ, máy trạm luôn được cập nhật mới nhất, thiết lập chế độ quét thường xuyên ít nhất là hàng tuần.

c. Lựa chọn, triển khai các phần mềm chống virus, thư rác trên các máy chủ, các thiết bị di động trong mạng và những hệ thống thông tin xung yếu như: cổng thông tin điện tử, thư điện tử, một cửa điện tử,... để phát hiện, loại trừ những đoạn mã độc hại (virus, trojan, worms,...) và hỗ trợ người sử dụng cài đặt các phần mềm này trên máy trạm.

2. Các đơn vị và cá nhân sử dụng hệ thống mạng máy tính có trách nhiệm:

a. Tuân thủ các biện pháp phòng và chống virus máy tính. Mọi dữ liệu từ các thiết bị lưu trữ bên ngoài và từ Internet đều phải được quét diệt virus trước khi sử dụng. Những máy tính phát hiện có virus phải được tách khỏi mạng về mặt vật lý để tránh tình trạng lây nhiễm sang các máy tính khác.

b. Khi phần mềm chống virus không còn hiệu lực cần thông báo ngay cho người quản trị hệ thống để có giải pháp xử lý thích hợp. Nghiêm cấm các cá nhân sử dụng máy tính chưa cài đặt phần mềm phòng diệt virus kết nối vào hệ thống mạng nội bộ của Bộ Tư pháp.

## Chương IV
## TỔ CHỨC THỰC HIỆN

### Điều 15. Xử lý vi phạm

Đơn vị và cá nhân vi phạm Quy chế này tuỳ theo tính chất, mức độ vi phạm thì 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, thiết bị, thông tin, dữ liệu trên hệ thống mạng máy tính của Bộ thì phải chịu trách nhiệm bồi thường theo quy định của pháp luật.

### Điều 16. Tổ chức thực hiện

Các đơn vị và cá nhân chịu trách nhiệm thi hành Quy chế này.

Thủ trưởng các đơn vị có trách nhiệm quán triệt, chỉ đạo và giám sát các cá nhân thuộc đơn vị mình thực hiện đúng nội dung Quy chế này.

Trong quá trình tổ chức thực hiện, nếu có những vấn đề khó khăn, vướng mắc, các đơn vị, cá nhân sử dụng cần phản ánh ngay với Cục Công nghệ thông tin để tổng hợp, trình Bộ trưởng xem xét, sửa đổi, bổ sung Quy chế cho phù hợp.

**BỘ TRƯỞNG**

Ký bởi: Bộ Tư pháp
Email: btp@moj.gov.vn
Cơ quan: Bộ Tư pháp

**Hà Hùng Cường**