BỘ KHOA HỌC VÀ CÔNG NGHỆ
CỤC SỞ HỮU TRÍ TUỆ

Số: 5033 /QĐ-SHTT

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

Hà Nội, ngày 21 tháng 10 năm 2022

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an toàn thông tin mạng và an ninh mạng

CỤC TRƯỞNG CỤC SỞ HỮU TRÍ TUỆ

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

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

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

Thông tư số 03/2017/TT-BTTTT ngày 24 tháng 4 năm 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 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

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

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 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 Quyết định số 1760/QĐ-BKHCN ngày 09 tháng 9 năm 2022 của Bộ trưởng Bộ Khoa học và Công nghệ ban hành Quy chế bảo đảm an toàn thông tin mạng và an ninh mạng;

Căn cứ Quyết định số 2525/QĐ-BKHCN ngày 04 tháng 9 năm 2018 của Bộ trưởng Bộ Khoa học và Công nghệ về việc ban hành Điều lệ Tổ chức và Hoạt động của Cục Sở hữu trí tuệ;

Theo đề nghị của Giám đốc Trung tâm Công nghệ thông tin.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn thông tin mạng và an ninh mạng.

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày ký.

Điều 3. Giám đốc Trung tâm Công nghệ thông tin, Thủ trưởng các đơn vị trực thuộc Cục Sở hữu trí tuệ và tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3 (để thực hiện);
- Trung tâm CNTT - Bộ KH&CN (để phối hợp);
- Cục trưởng, các Phó Cục trưởng (để chỉ đạo);
- Lưu: VT, CNTT(3).

CỤC TRƯỞNG

Đinh Hữu Phí

BỘ KHOA HỌC VÀ CÔNG NGHỆ
CỤC SỞ HỮU TRÍ TUỆ

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

QUY CHẾ
Bảo đảm an toàn thông tin mạng và an ninh mạng

(Kèm theo Quyết định số 5033 /QĐ-SHTT ngày 21 tháng 10 năm 2022 của Cục Sở hữu trí tuệ)

Chương I
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 bảo đảm an toàn thông tin mạng và an ninh mạng trong các hoạt động chuyển đổi số, ứng dụng công nghệ thông tin, vận hành, khai thác hệ thống, hạ tầng thông tin, phần mềm, dữ liệu thuộc phạm vi quản lý của Cục Sở hữu trí tuệ và các đơn vị trực thuộc Cục Sở hữu trí tuệ.

2. Đối tượng áp dụng

a) Các đơn vị trực thuộc Cục Sở hữu trí tuệ (sau đây gọi là "đơn vị"), công chức, viên chức và người lao động làm việc tại Cục Sở hữu trí tuệ (sau đây gọi là "cá nhân") có kết nối vào hệ thống mạng của Cục Sở hữu trí tuệ;

b) Cơ quan, tổ chức, cá nhân có kết nối vào hệ thống mạng của Cục Sở hữu trí tuệ;

c) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ công nghệ thông tin và an toàn thông tin mạng cho Cục Sở hữu trí tuệ.

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 số và các 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 việc bảo đảm thông tin trên mạng không gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

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

4. *Cổng thông tin điện tử* là điểm truy nhập duy nhất của Cục Sở hữu trí tuệ trên môi trường mạng, liên kết, tích hợp các kênh thông tin, các dịch vụ và các ứng dụng mà qua đó người dùng có thể khai thác, sử dụng và cá nhân hóa việc hiển thị thông tin.

5. *Mã độc* là đoạn mã hoặc 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.

6. *Mạng cục bộ (LAN - Local Area Network)* là một hệ thống mạng bao gồm các máy tính và các thiết bị ngoại vi được kết nối với nhau thông qua các thiết bị mạng để chia sẻ tài nguyên như thông tin, dữ liệu, phần mềm và các thiết bị ngoại vi.

7. *Dữ liệu nhạy cảm* là dữ liệu có thông tin mật, thông tin lưu hành nội bộ của Cục Sở hữu trí tuệ hoặc do Cục Sở hữu trí tuệ quản lý, nếu lộ lọt ra ngoài sẽ gây ảnh hưởng xấu đến danh tiếng, tài chính và hoạt động của Cục Sở hữu trí tuệ.

8. *Đơn vị vận hành hệ thống thông tin* là đơn vị được Cục trưởng Cục Sở hữu trí tuệ giao nhiệm vụ vận hành hệ thống thông tin. Trong trường hợp hệ thống thông tin thuê ngoài dịch vụ công nghệ thông tin, đơn vị vận hành hệ thống thông tin là bên cung cấp dịch vụ.

Điều 3. Nguyên tắc chung bảo đảm an toàn thông tin mạng và an ninh mạng

1. Bảo đảm an toàn thông tin mạng và an ninh mạng được thực hiện xuyên suốt, toàn bộ quá trình trong khâu thiết kế, xây dựng, mua sắm, nâng cấp, vận hành, bảo trì và ngừng sử dụng hạ tầng, hệ thống thông tin, phần mềm, dữ liệu.

2. Trách nhiệm bảo đảm an toàn thông tin mạng và an ninh mạng gắn với trách nhiệm của người đứng đầu cơ quan, đơn vị và cá nhân trực tiếp liên quan.

3. Trường hợp có văn bản, quy định cập nhật, thay thế hoặc quy định khác tại văn bản quy phạm pháp luật, quyết định của cấp có thẩm quyền cao hơn thì áp dụng quy định tại văn bản đó.

4. Thông tin thuộc Danh mục bí mật nhà nước được bảo vệ theo quy định của pháp luật về bảo vệ bí mật nhà nước.

5. Xử lý sự cố an toàn 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 và Điều 8 Luật An ninh mạng.

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 mạng nội bộ mà không có sự hướng dẫn hoặc đồng ý của đơn vị quản lý hệ thống thông tin; 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, thiết bị thu phát sóng wifi, thiết bị kết nối mạng internet vệ tinh).

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.

4. Cố ý tạo ra, cài đặt, phát tán mã độc gây ảnh hưởng đến hoạt động bình thường của hệ thống thông tin.

5. 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.

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

7. 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.

8. Cung cấp tài khoản có quyền trị cho cá nhân không đủ thẩm quyền.

Chương II
BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 5. Quản lý, sử dụng trang thiết bị công nghệ thông tin

1. Cá nhân và đơn vị có trách nhiệm bảo đảm an toàn thông tin mạng trong quản lý, sử dụng thiết bị công nghệ thông tin được giao.

2. Đối với trang thiết bị công nghệ thông tin có lưu trữ dữ liệu nhạy cảm khi thay đổi mục đích sử dụng hoặc thanh lý, Trung tâm Công nghệ thông tin phải thực hiện các biện pháp xóa, tiêu hủy dữ liệu đó đảm bảo không có khả năng phục hồi. Trường hợp không thể tiêu hủy được dữ liệu, Trung tâm Công nghệ thông tin phải thực hiện tiêu hủy cấu phần lưu trữ dữ liệu trên trang thiết bị công nghệ thông tin đó.

3. Trang thiết bị công nghệ thông tin 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 được tháo bộ phận lưu trữ khỏi thiết bị hoặc xóa thông tin, dữ liệu lưu trữ trên thiết bị (trừ trường hợp để khôi phục dữ liệu).

4. Trung tâm Công nghệ thông tin phân công cán bộ thực hiện việc quản lý, vận hành và định kỳ kiểm tra, phối hợp với Văn phòng Cục thực hiện việc sửa chữa, bảo trì thiết bị (bao gồm thiết bị đang hoạt động và thiết bị dự phòng).

Điều 6. Bảo đảm an toàn thông tin trong việc quản lý cán bộ, công chức, viên chức và người lao động

1. Các đơn vị trực thuộc Cục 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 thông tin của từng cá nhân trong đơn vị.

2. Khi công chức, viên chức và người lao động trong đơn vị chấm dứt hoặc thay đổi công việc, đơn vị phải:

a) Xác định rõ trách nhiệm của cá nhân và các bên liên quan trong việc quản lý, sử dụng các tài sản công nghệ thông tin đã được giao cho cá nhân sử dụng;

b) Văn phòng Cục lập biên bản bàn giao tài sản công nghệ thông tin;

c) Trung tâm Công nghệ thông tin thay đổi hoặc thu hồi quyền truy cập các hệ thống thông tin đối với cá nhân đó.

Điều 7. Bảo đảm an toàn hệ thống công nghệ thông tin

1. Bảo đảm an toàn thông tin đối với trung tâm dữ liệu/phòng máy chủ:

a) 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/phòng máy chủ và phải được thiết lập cơ chế bảo vệ, theo dõi phát hiện xâm nhập và biện pháp kiểm soát truy nhập, 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. Đơn vị vận hành trung tâm dữ liệu/phòng máy chủ có trách nhiệm xây dựng nội quy hoặc hướng dẫn làm việc khu vực này;

b) Trung tâm dữ liệu/phòng máy chủ là khu vực hạn chế tiếp cận. Chỉ những cá nhân có quyền, nhiệm vụ được giao theo quy định mới được phép vào trung tâm dữ liệu/phòng máy chủ. Việc vào, ra phòng máy chủ phải được kiểm soát bằng thiết bị bảo vệ (quẹt thẻ, vân tay, sinh trắc học, nhật ký vào ra,…);

c) Trung tâm dữ liệu/phòng máy chủ phải được trang bị hệ thống lưu điện đủ công suất và duy trì thời gian hoạt động của các máy chủ ít nhất 15 phút khi có sự cố mất điện;

d) Trung tâm dữ liệu/phòng máy chủ phải có hệ thống làm mát điều hòa không khí, độ ẩm để đảm bảo 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. Đơn vị phải cử cán bộ thường xuyên giám sát thiết bị, hạ tầng của trung tâm dữ liệu/phòng máy chủ.

2. Bảo đảm an toàn thông tin khi sử dụng máy tính:

a) Chỉ được cài đặt phần mềm hợp lệ và thuộc danh mục phần mềm được phép sử dụng do cơ quan có thẩm quyền ban hành trên máy tính của cá nhân được Cục cung cấp; cá nhân không được tự ý cài đặt hoặc gỡ bỏ các phần mềm khi chưa có sự đồng ý của Trung tâm Công nghệ thông tin; Trung tâm Công nghệ thông tin thường xuyên cập nhật phần mềm và hệ điều hành;

b) Trung tâm Công nghệ thông tin cài đặt phần mềm phòng, chống mã độc có bản quyền và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm; khi phát hiện bất kỳ dấu hiệu nào liên quan đến việc máy tính bị nhiễm phần mềm độc hại, người sử dụng phải tắt máy và báo trực tiếp cho Trung tâm Công nghệ thông tin để được xử lý kịp thời;

c) Chỉ truy cập 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; có trách nhiệm bảo mật tài khoản truy nhập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác.

3. Quản lý tài khoản truy cập:

a) Cá nhân sử dụng hệ thống thông tin được cấp và sử dụng tài khoản truy cập với định danh duy nhất gắn với cá nhân đó;

b) Trường hợp cá nhân thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ hưu, trong vòng không quá 05 ngày làm việc sau khi có quyết định của cấp có thẩm quyền thì đơn vị quản lý cá nhân đó phải thông báo Trung tâm công nghệ thông tin bằng văn bản có xác nhận của thủ trưởng đơn vị để điều chỉnh, thu hồi, hủy bỏ các quyền sử dụng đối với hệ thống thông tin;

c) 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 nhập của người sử dụng 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; nghiêm cấm cung cấp tài khoản quản trị hoặc gán thêm quyền quản trị cho người dùng thông thường;

d) Khi có yêu cầu khóa quyền truy cập hệ thống thông tin của tài khoản đang hoạt động, lãnh đạo đơn vị phải yêu cầu bằng văn bản gửi Trung tâm công nghệ thông tin để xem xét, thực hiện. Trung tâm Công nghệ 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;

đ) Việc quản lý tài khoản thư điện tử của Cục Sở hữu trí tuệ thực hiện theo quy định tại Chương III của Quy chế quản lý và sử dụng hệ thống công nghệ thông tin của Cục Sở hữu trí tuệ được ban hành kèm theo Quyết định số 5032/QĐ-SHTT

ngày 21/10/2022. Công tác phòng chống thư rác được thực hiện theo quy định tại Nghị định số 91/2020/NĐ-CP ngày 14/8/2020 và hướng dẫn tại Thông tư số 22/2021/TT-BTTTT ngày 13/12/2021.

4. Bảo đảm an toàn thông tin mức ứng dụng:

a) 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;

b) Phần mềm, ứng dụng phải đáp ứng các yêu cầu sau: cấu hình phần mềm, ứng dụng để xác thực người sử dụng; giới hạn thời gian để chờ đóng phiên kết nối; mã hóa thông tin xác thực trên hệ thống; không khuyến khích việc đăng nhập tự động;

c) Thiết lập, phân quyền truy nhập, quản trị, sử dụng tài nguyên khác nhau của phần mềm, ứng dụng với người sử dụng/nhóm người sử dụng 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;

d) 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 công nghệ thông tin quản lý;

đ) 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.

5. Bảo đảm an toàn thông tin mức dữ liệu:

a) Trung tâm Công nghệ 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, cơ sở dữ liệu. Đơn vị phải bố trí máy tính riêng không kết nối mạng, đặt mật khẩu, mã hóa dữ liệu và các biện pháp bảo mật khác bảo đảm an toàn thông tin để soạn thảo, lưu trữ dữ liệu, thông tin và tài liệu quan trọng ở các mức độ mật, tuyệt mật, tối mật;

b) Các đơn vị trực thuộc Cục phải thường xuyên nâng cao nhận thức của cá nhân trong đơn vị trong hoạt động chia sẻ, gửi, nhận thông tin trên môi trường mạng cần phải sử dụng mật khẩu để bảo vệ thông tin;

c) Đối với hoạt động trao đổi thông tin, dữ liệu với bên ngoài, đơn vị và cá nhân thực hiện trao đổi thông tin, dữ liệu ra bên ngoài cam kết và có biện pháp bảo mật thông tin, dữ liệu được trao đổi. 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;

d) Các đơn vị, cá nhân không được phép cung cấp thông tin, dữ liệu về các đơn sở hữu công nghiệp chưa được công bố cho các tổ chức, cá nhân không có trách nhiệm liên quan dưới mọi hình thức.

Điều 8. Xác định cấp độ và phương án bảo đảm an toàn hệ thống thông tin

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.

2. 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 số 85/2016/NĐ-CP.

Điều 9. Quy trình ứng cứu sự cố an toàn thông tin mạng

1. Đơn vị, cá nhân khi phát hiện dấu hiệu tấn công hoặc sự cố an toàn thông tin mạng cần nhanh chóng báo cho Trung tâm Công nghệ thông tin để tổng hợp, báo cáo Lãnh đạo Cục.

2. Khi xảy ra sự cố an toàn thông tin mạng thuộc loại hình tấn công mạng, Trung tâm Công nghệ thông tin thực hiện báo cáo theo quy định tại Điểm a Khoản 1 Điều 11 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 và Điều 9 Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc. Trách nhiệm của các đơn vị, cá nhân 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 số 05/2017/QĐ-TTg và Điều 10 Thông tư số 20/2017/TT-BTTTT.

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

Chương III
TỔ CHỨC THỰC HIỆN

Điều 10. Kinh phí thực hiện

Kinh phí bảo đảm an toàn thông tin mạng và an ninh mạng được lấy từ nguồn ngân sách nhà nước dự toán hằng năm của Cục Sở hữu trí tuệ.

Điều 11. Khen thưởng, kỷ luật

1. Kết quả thực hiện Quy chế này là một trong những tiêu chí có thể được sử dụng để đánh giá kết quả thực hiện công việc hằng năm của cá nhân, đơn vị.

2. Đơn vị, cá nhân vi phạm Quy chế này và các quy định khác của pháp luật về bảo đảm an toàn thông tin mạng và an ninh 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, thiết bị, thông tin, dữ liệu thì chịu trách nhiệm bồi thường theo pháp luật hiện hành.

Điều 12. Trách nhiệm thi hành

1. Giám đốc Trung tâm Công nghệ thông tin giúp Cục trưởng theo dõi việc triển khai và thực hiện Quy chế này.

2. Thủ trưởng các đơn vị trực thuộc Cục có trách nhiệm phổ biến, quán triệt đến toàn bộ cán bộ, nhân viên trong đơn vị thực hiện các quy định của Quy chế này.

3. Công chức, viên chức, người lao động của Cục có trách nhiệm tuân thủ Quy chế; thông báo các vấn đề bất thường liên quan tới an toàn thông tin mạng cho Trung tâm Công nghệ thông tin; chịu trách nhiệm trước pháp luật và Lãnh đạo Cục về các vi phạm, làm thất thoát dữ liệu mật do không tuân thủ Quy chế.

4. Trong quá trình thực hiện, nếu có những vấn đề khó khăn, vướng mắc, các đơn vị phản ánh về Trung tâm Công nghệ thông tin để tổng hợp, trình Cục trưởng xem xét, sửa đổi, bổ sung quy chế./.