VIỆN KIỂM SÁT NHÂN DÂN TỐI CAO	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 245 /QĐ-VKSTC	*Hà Nội, ngày 29 tháng 7 năm 2021*

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an toàn, an ninh thông tin mạng của Viện kiểm sát nhân dân

VIỆN TRƯỞNG VIỆN KIỂM SÁT NHÂN DÂN TỐI CAO

Căn cứ Luật Tổ chức Viện kiểm sát nhân dân năm 2014;

Căn cứ Luật Công nghệ thông tin năm 2006 (sửa đổi, bổ sung năm 2017);

Căn cứ Luật An toàn thông tin mạng năm 2015;

Căn cứ Luật An ninh mạng năm 2018;

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

Căn cứ Chỉ thị số 02/CT-TTg ngày 04/7/2018 của Thủ tướng Chính phủ về công tác bảo vệ bí mật nhà nước trên không gian mạng;

Căn cứ Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông về việc 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;

Xét đề nghị của Cục trưởng Cục Thống kê tội phạm và 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 của Viện kiểm sát nhân dân.

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

Điều 3. Thủ trưởng các đơn vị thuộc Viện kiểm sát nhân dân tối cao, Viện trưởng Viện kiểm sát quân sự trung ương, Viện trưởng Viện kiểm sát nhân dân cấp cao, Viện trưởng Viện kiểm sát nhân dân cấp tỉnh, thành phố trực thuộc trung ương, Viện trưởng Viện kiểm sát nhân dân cấp huyện chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Các đ/c Phó Viện trưởng VKSNDTC;
- Như Điều 3 (để thực hiện);
- Lưu: VT, Cục 2.

VIỆN TRƯỞNG

VIỆN KIỂM SÁT NHÂN DÂN TỐI CAO

Lê Minh Trí

QUY CHẾ
BẢO ĐẢM AN TOÀN, AN NINH THÔNG TIN MẠNG CỦA VIỆN KIỂM SÁT NHÂN DÂN

(Ban hành kèm theo Quyết định số 245./QĐ-VKSTC ngày 29./..7.../2021 của Viện trưởng Viện kiểm sát nhân dân tối cao)

Chương I
QUY ĐỊNH CHUNG

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

1. Quy chế này quy định nguyên tắc, nội dung bảo đảm và trách nhiệm của các cơ quan, tổ chức, cá nhân về bảo đảm an toàn, an ninh thông tin mạng trong hệ thống Viện kiểm sát nhân dân.

2. Quy chế này áp dụng đối với:

a) Viện kiểm sát nhân dân tối cao, Viện kiểm sát nhân dân cấp dưới;

b) Công chức, viên chức, người lao động trong Viện kiểm sát nhân dân;

c) Cơ quan, tổ chức, cá nhân tham gia quản lý, vận hành, cung cấp dịch vụ công nghệ thông tin cho Viện kiểm sát nhân dân; tổ chức, cá nhân sử dụng hệ thống mạng của Viện kiểm sát nhân dân;

d) Viện trưởng Viện kiểm sát quân sự trung ương quy định cụ thể việc bảo đảm an toàn, an ninh thông tin mạng trong hệ thống Viện kiểm sát quân sự.

Điều 2. Từ ngữ sử dụng trong Quy chế

Các thuật ngữ: an toàn thông tin mạng, an ninh thông tin mạng, hạ tầng kỹ thuật, trang thông tin điện tử, cổng thông tin điện tử, phần mềm độc hại, mạng LAN, trung tâm dữ liệu, hệ thống thông tin, đơn vị vận hành hệ thống thông tin… trong Quy chế này được thực hiện theo quy định tại Luật an toàn thông tin mạng và pháp luật khác có liên quan.

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

1. Các quy định về bảo đảm an toàn, an ninh thông tin mạng phải thực hiện nghiêm theo quy định của pháp luật có liên quan.

2. Bảo đảm an toàn, an ninh thông tin mạng là yêu cầu bắt buộc, thường xuyên, liên tục, xuyên suốt quá trình thiết kế, xây dựng, vận hành, nâng cấp, hủy bỏ hệ thống thông tin.

3. Xử lý sự cố an toàn, an ninh thông tin mạng 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

Ngoài các hành vi bị nghiêm cấm theo quy định của Luật an ninh mạng và các văn bản pháp luật khác, thì các hành vi sau đây bị nghiêm cấm:

1. Nghiêm cấm soạn thảo, lưu trữ, sao chụp thông tin bí mật nhà nước trên máy tính hoặc thiết bị khác có tính năng lưu trữ thông tin có kết nối Internet; kết nối vật lý hệ thống mạng nội bộ chứa thông tin bí mật nhà nước với mạng Internet và ngược lại.

2. 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.

3. Nghiêm cấm sử dụng thiết bị nhớ ngoài USB, ổ cứng di động và các thiết bị, phương tiện điện tử có khả năng lưu trữ dữ liệu khác để sao chép dữ liệu giữa các máy tính soạn thảo nội dung bí mật nhà nước với máy tính hoặc thiết bị, phương tiện điện tử có kết nối Internet.

4. Tự ý đấu nối thiết bị cấp phát địa chỉ mạng và thiết bị khác vào mạng nội bộ mà không được sự đồng ý của đơn vị chuyên trách về an toàn, an ninh thông tin mạng.

5. Sử dụng hệ thống mạng của Viện kiểm sát nhân dân để thực hiện hành vi bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của cơ quan, cá nhân.

Chương II
NỘI DUNG BẢO ĐẢM AN TOÀN, AN NINH THÔNG TIN MẠNG

Điều 5. Chủ quản hệ thống thông tin

1. Viện kiểm sát nhân dân tối cao là chủ quản hệ thống thông tin do Viện kiểm sát nhân dân tối cao quyết định đầu tư xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin.

2. Các đơn vị thuộc Viện kiểm sát nhân dân tối cao, Viện kiểm sát nhân dân cấp dưới là chủ quản hệ thống thông tin do đơn vị quyết định đầu tư xây dựng, thiết lập, nâng cấp, mở rộng.

3. Chủ quản hệ thống thông tin có thẩm quyền bảo đảm an toàn, an ninh thông tin mạng theo quy định của pháp luật liên quan và theo quy định của Quy chế này.

Điều 6. Đơn vị chuyên trách về an toàn, an ninh thông tin mạng

1. Cục Thống kê tội phạm và Công nghệ thông tin là đơn vị chuyên trách

về an toàn, an ninh thông tin mạng của cơ quan Viện kiểm sát nhân dân tối cao và của Viện kiểm sát nhân dân cấp dưới.

2. Đơn vị chuyên trách về công nghệ thông tin tại các đơn vị trực thuộc Viện kiểm sát nhân dân tối cao có hệ thống thông tin do đơn vị quyết định đầu tư xây dựng, thiết lập là đơn vị chuyên trách về an toàn, an ninh thông tin mạng của đơn vị mình.

3. Đơn vị chuyên trách về công nghệ thông tin tại Viện kiểm sát nhân dân cấp cao là đơn vị chuyên trách về an toàn, an ninh thông tin mạng của đơn vị mình và các đơn vị trực thuộc.

4. Đơn vị chuyên trách về công nghệ thông tin tại Viện kiểm sát nhân dân cấp tỉnh là đơn vị chuyên trách về an toàn, an ninh thông tin mạng của đơn vị mình và cấp dưới trực thuộc.

5. Đơn vị chuyên trách về an toàn, an ninh thông tin mạng có thẩm quyền bảo đảm an toàn, an ninh thông tin mạng theo quy định của pháp luật liên quan và theo quy định của Quy chế này.

Điều 7. Về người sử dụng hệ thống thông tin mạng trong Viện kiểm sát nhân dân

1. Các đơn vị có trách nhiệm bảo đảm an toàn, an ninh thông tin mạng của đơn vị mình; căn cứ quy mô, chức năng, điều kiện thực tế của đơn vị để bố trí nhân sự chuyên trách chịu trách nhiệm bảo đảm an toàn, an ninh thông tin mạng cho phù hợp; 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 toàn, an ninh thông tin mạng.

2. Công chức, viên chức và người lao động trong Viện kiểm sát nhân dân có trách nhiệm bảo đảm an toàn, an ninh thông tin mạng trong phạm vi xử lý công việc của mình theo quy định của Nhà nước và của Viện kiểm sát nhân dân.

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

1. Chủ quản hệ thống thông tin có trách nhiệm xác định cấp độ hệ thống thông tin và xây dựng phương án bảo đảm hệ thống thông tin theo cấp độ phục vụ mục đích đánh giá an toàn, an ninh thông tin mạng và bảo đảm an toàn, an ninh thông tin mạng cho các hệ thống thông tin của đơn vị mình.

2. Đơn vị chuyên trách về an toàn, an ninh thông tin mạng có trách nhiệm thực hiện thẩm định hồ sơ đề xuất cấp độ căn cứ trên các nguyên tắc quy định của pháp luật.

3. Phương án bảo đảm an toàn, an ninh hệ thống thông tin

a) Phương án bảo đảm an toàn, an ninh hệ thống thông tin mạng phải phù hợp với cấp độ của hệ thống thông tin và đáp ứng yêu cầu quy định của pháp luật, các tiêu chuẩn, quy chuẩn kỹ thuật khác;

b) Đơn vị chuyên trách về an toàn, an ninh thông tin mạng thuộc đơn vị chịu trách nhiệm giám sát việc triển khai các phương án bảo đảm an toàn, an ninh thông tin mạng đã được phê duyệt.

Điều 9. Bảo đảm an toàn, an ninh thông tin tại Trung tâm dữ liệu

1. Các thiết bị kết nối mạng, thiết bị bảo mật quan trọng như tường lửa, thiết bị định tuyến, hệ thống máy chủ, hệ thống lưu trữ... phải được đặt trong Trung tâm dữ liệu 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.

2. Trung tâm dữ liệu phải có 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; 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.

3. Chỉ những cá nhân có quyền, nhiệm vụ theo quy định của thủ trưởng đơn vị mới được phép vào, ra Trung tâm dữ liệu. Việc vào, ra Trung tâm dữ liệu phải được kiểm soát bằng thiết bị bảo vệ (quẹt thẻ, vân tay, sinh trắc học, ...).

4. Đối với phần mềm thương mại tại Trung tâm dữ liệu yêu cầu phải có bản quyền.

Điều 10. Bảo đảm an toàn, an ninh thông tin đối với hệ thống mạng

1. Hệ thống mạng nội bộ (LAN) phải được thiết kế phân vùng theo chức năng cơ bản, bao gồm: vùng mạng người dùng; vùng mạng kết nối hệ thống ra bên ngoài Internet và các mạng khác; vùng mạng máy chủ công cộng; vùng mạng máy chủ nội bộ; vùng mạng máy chủ cơ sở dữ liệu, vùng mạng máy chủ quản trị. Dữ liệu trao đổi giữa các vùng mạng phải được quản lý, giám sát bởi hệ thống các thiết bị mạng, thiết bị bảo mật.

2. Đơn vị trực thuộc tham gia kết nối, sử dụng hệ thống mạng nội bộ có trách nhiệm bảo đảm an toàn, an ninh thông tin đối với hệ thống mạng nội bộ và các thiết bị của mình khi thực hiện kết nối vào mạng nội bộ; thông báo sự cố hoặc

các hành vi phá hoại, xâm nhập bất hợp pháp về đơn vị chuyên trách về an toàn, an ninh thông tin mạng để xử lý; không được tìm cách truy cập dưới bất cứ hình thức nào vào các khu vực không được phép truy cập.

3. Các hệ thống cáp mạng máy tính phải được lắp đặt trong ống, máng che đậy kín, hạn chế khả năng tiếp cận trái phép.

Điều 11. Bảo đảm an toàn, an ninh thông tin đối với thiết bị kết nối mạng

1. Trang thiết bị công nghệ thông tin có lưu trữ thông tin lưu hành nội bộ của đơn vị hoặc do đơn vị quản lý khi thay đổi mục đích sử dụng hoặc thanh lý, đơn vị phải thực hiện các biện pháp xóa, tiêu hủy dữ liệu đó bảo đảm không có khả năng phục hồi.

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

3. Khi phát hiện bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy tính, thiết bị kết nối mạng máy tính thì phải tắt máy và báo trực tiếp cho đơn vị chuyên trách về an toàn, an ninh thông tin mạng để được xử lý kịp thời.

Điều 12. Quản lý tài khoản truy cập

1. 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, chỉ truy cập vào các trang/cổng thông tin điện tử, ứng dụng trực tuyến và các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình; có trách nhiệm bảo mật tài khoản truy cập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác.

2. Tài khoản quản trị hệ thống (mạng máy tính, 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 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.

3. Đơn vị chuyên trách về an toàn, an ninh thông tin mạng khóa quyền truy cập của tài khoản các hệ thống thông tin 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 mạng.

4. 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 cơ quan, đơn vị quản lý cá nhân đó phải thông báo cơ quan, đơn vị chuyên trách về an toàn, an ninh thông tin mạng để điều chỉnh, thu hồi, hủy bỏ các quyền sử dụng đối với hệ thống thông tin.

Điều 13. Bảo đảm an toàn, an ninh thông tin đối với việc xây dựng và sử dụng phần mềm ứng dụng

1. Yêu cầu về bảo đảm an toàn, an ninh 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 sử dụng; 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 được để chế độ đăng nhập tự động.

3. Phần mềm ứng dụng cần được kiểm tra phát hiện và khắc phục các điểm yếu về an toàn, an ninh thông tin mạng trước khi đưa vào sử dụng và trong quá trình sử dụng.

4. Cá nhân chỉ sử dụng phần mềm do đơn vị chuyên trách về an toàn, an ninh thông tin mạng cài đặt trên máy tính, thiết bị kết nối mạng máy tính được cấp; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm khi chưa có sự đồng ý của đơn vị chuyên trách về an toàn, an ninh thông tin mạng.

5. Thiết lập, phân quyền truy cập, 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.

6. Chỉ cho phép sử dụng các giao thức mạng có hỗ trợ chức năng mã hóa thông tin (SSH, SSL, VPN hoặc tương đương) khi truy cập, 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.

Điều 14. Bảo đảm an toàn, an ninh thông tin đối với dữ liệu

1. Chủ quản hệ thống thông tin phải 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.

2. Tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ phải được sao lưu dự phòng định kỳ và lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng.

3. Đơn vị cần 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, an ninh 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.

Điều 15. 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, chủ quản 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, chủ quản hệ thống thông tin 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. Trong quá trình vận hành hệ thống thông tin, 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.

4. Chủ quản hệ thống thông tin phải thực hiện công tác bảo đảm an toàn, an ninh thông tin mạng, 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 khi xây dựng, nâng cấp phần mềm ứng dụng.

Điều 16. Giám sát an toàn, an ninh thông tin mạng

1. Các hệ thống thông tin bắt buộc phải có chức năng 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 cập 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.

2. Đơn vị chuyên trách về an toàn, an ninh thông tin mạng 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; việc chia sẻ, gửi, nhận thông tin trên môi trường mạng cần phải sử dụng mật khẩu để bảo vệ thông tin.

3. 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 phải cam kết và có biện

pháp bảo mật thông tin, dữ liệu được trao đổi. Giao dịch điện tử 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.

4. Nguyên tắc, yêu cầu, nội dung, phương thức, hệ thống kỹ thuật phục vụ công tác giám sát thực hiện theo quy định của pháp luật về hoạt động giám sát an toàn hệ thống thông tin.

Điều 17. Ứng cứu sự cố an toàn, an ninh thông tin mạng

1. Các đơn vị, cá nhân khi phát hiện dấu hiệu tấn công hoặc sự cố an toàn, an ninh thông tin mạng cần nhanh chóng báo cho đơn vị chuyên trách về an toàn, an ninh thông tin mạng.

2. Khi xảy ra sự cố an toàn, an ninh thông tin mạng thuộc loại hình tấn công mạng, đơn vị vận hành hệ thống thông tin thực hiện báo cáo đơn vị chuyên trách về an toàn, an ninh thông tin mạng để khắc phục, xử lý kịp thời.

Điều 18. Kiểm tra, đánh giá, chế độ báo cáo an toàn, an ninh thông tin mạng

1. Nội dung kiểm tra, đánh giá:

a) Kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn, an ninh thông tin theo cấp độ;

b) Đánh giá hiệu quả của biện pháp bảo đảm an toàn, an ninh hệ thống thông tin;

c) Đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống;

d) Kiểm tra, đánh giá khác do chủ quản hệ thống thông tin quy định.

2. Hình thức kiểm tra, đánh giá:

a) Kiểm tra, đánh giá định kỳ theo kế hoạch của chủ quản hệ thống thông tin;

b) Kiểm tra, đánh giá đột xuất theo yêu cầu của cấp có thẩm quyền.

3. Chế độ báo cáo

a) Đơn vị vận hành hệ thống thông tin hàng năm định kỳ hoặc đột xuất báo cáo công tác thực thi bảo đảm an toàn hệ thống thông tin theo chủ quản hệ thống thông tin hoặc cơ quan quản lý nhà nước chuyên ngành có thẩm quyền.

b) Báo cáo định kỳ gửi về Cục Thống kê tội phạm và Công nghệ thông tin trước ngày 30 tháng 11 hàng năm để tổng hợp báo cáo lãnh đạo Viện kiểm sát nhân dân tối cao.

Điều 19. Kinh phí thực hiện

1. Kinh phí thực hiện yêu cầu về bảo đảm an toàn, an ninh thông tin theo cấp độ từ nguồn vốn ngân sách nhà nước.

2. Kinh phí đầu tư cho bảo đảm an toàn, an ninh thông tin mạng sử dụng vốn đầu tư công thực hiện theo quy định của Luật đầu tư công. 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, đánh giá, 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 cân đối bố trí trong dự toán ngân sách hàng năm.

Điều 20. Xử lý vi phạm

Đơn vị, cá nhân thuộc đối tượng áp dụng của Quy chế này vi phạm Quy chế và các quy định 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, thiết bị, thông tin, dữ liệu thì chịu trách nhiệm bồi thường theo pháp luật hiện hành.

Chương III

ĐIỀU KHOẢN THI HÀNH

Điều 21. Hiệu lực thi hành

Quy chế này có hiệu lực thi hành kể từ ngày ký Quyết định ban hành. Các quy định trước đây trái với Quy chế này bị bãi bỏ.

Điều 22. Trách nhiệm thực hiện

1. Thủ trưởng đơn vị thuộc Viện kiểm sát nhân dân tối cao, Viện trưởng Viện kiểm sát nhân dân và Viện kiểm sát quân sự các cấp chịu trách nhiệm tổ chức thực hiện Quy chế này.

2. Giao Cục Thống kê tội phạm và Công nghệ thông tin chủ trì, phối hợp với Văn phòng Viện kiểm sát nhân dân tối cao và các đơn vị có liên quan theo dõi, đôn đốc, hướng dẫn, kiểm tra việc thực hiện Quy chế này.

3. Trong quá trình thực hiện, nếu có khó khăn vướng mắc hoặc phát sinh những vấn đề cần phải sửa đổi, bổ sung thì kịp thời báo cáo Viện kiểm sát nhân dân tối cao qua Cục Thống kê tội phạm và Công nghệ thông tin để tổng hợp, báo cáo Viện trưởng Viện kiểm sát nhân dân tối cao xem xét, quyết định./.