HỌC VIỆN CHÍNH TRỊ QUỐC GIA
HỒ CHÍ MINH
HỌC VIỆN BÁO CHÍ VÀ TUYÊN TRUYỀN

ĐẢNG CỘNG SẢN VIỆT NAM

Số: 6346 -QĐ/HVBCTT

Hà Nội, ngày 16 tháng 12 năm 2021

QUYẾT ĐỊNH

Ban hành Quy chế Đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin tại Học viện Báo chí và Tuyên truyền

Căn cứ Luật Công nghệ thông tin số 67/2009/QH11 ngày 29/6/2006;

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về Ứng dụng Công nghệ thông tin trong hoạt động của cơ quan Nhà nước;

Căn cứ Quyết định số 6591/QĐ-HVCTQG ngày 01/11/2018 của Giám đốc Học viện chính trị Quốc gia Hồ Chí Minh về chức năng, nhiệm vụ, quyền hạn tổ chức bộ máy của Học viện Báo chí và Tuyên truyền;

Theo đề nghị của Văn phòng.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này "**Quy chế Đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin tại Học viện Báo chí và Tuyên truyền**".

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

Điều 3. Chánh Văn phòng, Bộ phận CNTT, Thủ trưởng các đơn vị thuộc Học viện Báo chí và Tuyên truyền chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Ban GĐ;
- Lưu: VP, CNTT.

GIÁM ĐỐC

HỌC VIỆN BÁO CHÍ VÀ TUYÊN TRUYỀN

Phạm Minh Sơn

HỌC VIỆN CHÍNH TRỊ QUỐC GIA
HỒ CHÍ MINH
HỌC VIỆN BÁO CHÍ VÀ TUYÊN TRUYỀN

ĐẢNG CỘNG SẢN VIỆT NAM

Hà Nội, ngày tháng năm 2021

QUY CHẾ
Đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin tại Học viện Báo chí và Tuyên truyền

(Ban hành kèm theo Quyết định số: QĐ/HVBCTT ngày tháng năm 2021 của Giám đốc Học viện)

CHƯƠNG I
NHỮNG QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh đối tượng áp dụng

1. Quy chế này quy định về nội dung, biện pháp đảm bảo an toàn, an ninh thông tin trong lĩnh vực ứng dụng công nghệ thông tin phục vụ cho công tác quản lý, điều hành tại Học viện Báo chí và Tuyên truyền.

2. Đối tượng áp dụng đối với các đơn vị trực thuộc Học viện Báo chí và Tuyên truyền và cán bộ, công chức, viên chức, giảng viên, nghiên cứu viên, người lao động, sinh viên, học viên (sau đây gọi là cá nhân) tham gia vào hoạt động ứng dụng công nghệ thông tin tại Học viện Báo chí và Tuyên truyền.

Điều 2. Giải thích từ ngữ

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

1. Bảo đảm an toàn thông tin: là sự bảo vệ thông tin và các hệ thống thông tin 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. Xâm phạm an toàn thông tin: Là hành vi truy nhập, sử dụng, tiết lộ, làm gián đoạn, sửa đổi, làm sai lệch chức năng, hủy hoại trái phép thông tin và hệ thống thông tin.

3. Hạ tầng kỹ thuật: Là tập hợp các thiết bị phần cứng, thiết bị lưu trữ, thiết bị ngoại vi, thiết bị kết nối mạng, thiết bị phụ trợ, đường truyền, mạng nội bộ, mạng diện rộng.

4. Hệ thống thông tin: Là cơ sở dữ liệu, tập hợp phần cứng, phần mềm 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 môi trường mạng.

5. Trang thông tin điện tử (trang thông tin tuyển sinh, trang thông tin sinh viên, thư viện số, thư viện điện tử...): là trang thông tin hay một tập hợp trang thông tin trên môi trường mạng phụ vụ cho việc cung cấp, trao đổi thông tin internet.

6. Cổng thông tin điện tử: Là điểm truy cập duy nhất của cơ quan đơn vị 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.

7. 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 trên hệ thống thông tin.

8. Bản ghi nhật ký hệ thống: Là một tập tin được tạo ra trên mỗi thiết bị của hệ thống thông tin như: thiết bị bảo mật, thiết bị tính toán, máy chủ ứng dụng.... có chứa tất cả các thông tin về các hoạt động xảy ra trên thiết bị đó, bản ghi nhật ký hệ thống dùng để phân tích những sự kiện xảy ra, nguồn gốc và các kết quả để có biện pháp thích hợp.

9. Thiết bị lưu trữ dữ liệu di động: Là các thiết bị để đọc, ghi dữ liệu có thể được di chuyển tới nhiều nơi, nhiều người có thể sử dụng (ổ cứng di động, USB, máy tính xách tay, thẻ nhớ, đĩa CD, DVD,...)

10. Lưu trữ trên môi trường mạng: Là phương thức lưu trữ sử dụng các ứng dụng lưu trữ của nhà cung cấp. Dữ liệu được đưa lên máy chủ của nhà cung cấp dịch vụ lưu trữ.

11. Người sử dụng: là cá nhân sử dụng máy tính, thiết bị di động có thể truy cập vào hệ thống mạng, hệ thống thông tin của Học viện.

Điều 3. Tài nguyên thông tin cần đảm bảo an toàn thông tin

Gồm các thành phần sau:

1. Hệ thống hạ tầng kỹ thuật:

a, Mạng kết nối internet của Học viện, mạng nội bộ (LAN) và các thiết bị kết nối mạng, thiết bị bảo mật, thiết bị phụ trợ.

b, Thiết bị tính toán, lưu trữ (máy chủ, máy trạm....).

c, Thiết bị ngoại vi (máy in, máy quét và các thiết bị số hóa, thiết bị lưu trữ dữ liệu di động,...).

d, Thiết bị công nghệ thông tin được kết nối mạng tại Học viện.

2. Phần mềm ứng dụng và cơ sở dữ liệu:

a, Trang/cổng thông tin điện tử của Học viện và các đơn vị.

b, Phần mềm, ứng dụng phục vụ công tác quản lý, điều hành các hoạt động của Học viện và các đơn vị.

c, Phần mềm, ứng dụng cung cấp dịch vụ trực tuyến.

d, Các dịch vụ mạng.

e, Cơ sở dữ liệu dùng chung.

3. Thông tin, dữ liệu được trao đổi, truyền tải, xử lý và lưu trữ trên hạ tầng kỹ thuật của Học viện.

Điều 4. Nguyên tắc chung về bảo đảm an toàn thông tin

1. Bảo đảm an toàn thông tin là yêu cầu bắt buộc, có tính xuyên suốt và phải thường xuyên liên, tục trong qúa trình:

a, Thu thập, tạo lập, xử lý, truyền tải, lưu trữ và sử dụng thông tin, dữ liệu.

b, Thiết kế, xây dựng, vận hành, nâng cấp, cải tiến, hủy bỏ hệ thống thông tin.

2. Các đơn vị và cá nhân có trách nhiệm thực hiện đầy đủ, nghiêm túc các quy định của pháp luật, quy chế của Học viện Báo chí và Tuyên truyền về bảo đảm an toàn thông tin.

3. Khi thực hiện thuê hoặc sử dụng dịch vụ công nghệ thông tin do bên thứ ba cung cấp, đơn vị và cá nhân phải quản lý việc sở hữu thông tin, dữ liệu từ dịch vụ đó; yêu cầu nhà cung cấp dịch vụ có trách nhiệm bảo mật thông tin; không để nhà cung cấp dịch vụ truy nhập, sử dụng thông tin, dữ liệu mà chưa có sự cho phép của cá nhân, đơn vị và Học viện.

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

Điều 5. Các hành vi bị nghiêm cấm

1. Vi phạm các quy định, quy trình về quản lý, vận hành, sử dụng và bảo đảm an toàn thông tin đối với hệ thống thông tin của Học viện.

2. Truy nhập, tác động trái phép, làm sai lệch, gây nguy hại đến thông tin, dữ liệu hoặc xâm phạm an toàn thông tin của Học viện và cá nhân.

3. Tấn công, làm ảnh hưởng đến hoạt động bình thường của hệ thống thông tin hoặc ngăn chặn trái phép, gây gián đoạn truy cập hợp pháp của người sử dụng tới hệ thống thông tin.

4. Sử dụng tài nguyên thông tin của Học viện để phát tán thư rác, tin nhắn rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo.

CHƯƠNG II
CÔNG TÁC BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 6. Bảo đảm an toàn thông tin mức vật lý

1. Bảo đảm an toàn thông tin mức vật lý là việc bảo vệ hạ tầng kỹ thuật, phần mềm ứng dụng và cơ sở dữ liệu khỏi các mối nguy hiểm vật lý (như: cháy, nổ, nhiệt độ, độ ẩm ngoài mức cho phép; thiên tai; mất điện; tác động cơ học) có thể gây ảnh hưởng đến hoạt động hệ thống.

2. Các biện pháp cơ bản bảo đảm an toàn thông tin mức vật lý bao gồm:

a, Quản lý phòng máy chủ:

- 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 phòng máy chủ;

- Phòng máy chủ 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 đối với từng khu

vực; máy chủ và hệ thống lưu trữ; tủ mạng và đấu nối; thiết bị nguồn điện và dự phòng điện khẩn cấp; vận hành, kiểm soát, quản trị hệ thống:

- Quá trình vào, ra phòng máy chủ phải được ghi nhận vào nhật ký quản lý phòng máy chủ. Chỉ những cá nhân có quyền, nhiệm vụ theo quy định của thủ trưởng đơn vị mới được phép vào phòng máy chủ. Trang bị cơ chế kiểm tra xác thực nâng cao (thẻ, vân tay,...) khi cần thiết.

- Có phương án, kế hoạch phòng, chống và khắc phục sự cố ngập đột nước, sét, cháy nổ; áp dụng các quy chuẩn kỹ thuật về an toàn kỹ thuật nhiệt, độ ẩm, ánh sáng cho các thiết bị tính toán, lưu trữ; bảo đảm các điều kiện hoạt động ổn định cho các hệ thống hỗ trợ như máy điều hòa nhiệt độ, nguồn cấp điện, dây dẫn;

- 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 10 phút khi có sự cố mất điện.

b, Thiết lập cơ chế dự phòng đối với các thiết bị hạ tầng kỹ thuật quan trọng: có kế hoạch kiểm tra, bảo dưỡng định kỳ và duy trì thông số kỹ thuật các thiết bị này hoặc có phương án sửa chữa, thay thế đáp ứng yêu cầu về độ sẵn sàng trong suốt thời gian lắp đặt, sử dụng.

c, Các đường truyền dữ liệu, đường truyền internet và hệ thống dây dẫn các mạng LAN, WAN phải được lắp đặt trong ống, máng che đậy kín, hạn chế khả năng tiếp cận trái phép.

d, Cá nhân sử dụng thiết bị lưu trữ dữ liệu di động để lưu trữ thông tin, dữ liệu của đơn vị mình có trách nhiệm bảo vệ thiết bị này và thông tin lưu trên thiết bị, tránh làm mất hoặc lộ thông tin, dữ liệu. Không mang ra nước ngoài thông tin, dữ liệu của đơn vị, của Nhà nước mà không liên quan tới nội dung công việc thực hiện ở nước ngoài.

e, Thiết bị tính toán có bộ phận lưu trữ hoặc thiết bị lưu trữ có chứa dữ liệu cần bảo vệ khi mang đi bảo hành, bảo dưỡng sửa chữa bên ngoài hoặc ngừng sử dụng phải được tháo bộ phận lưu trữ ra khỏi thiết bị hoặc xóa thông tin, dữ liệu lưu trữ trên thiết bị (trừ trường hợp để khôi phục dữ liệu). Khi thanh lý thiết bị thì phải xóa nội dung lưu trữ bằng phần mềm hoặc thiết bị hủy dữ liệu chuyên dụng hay phá hủy vật lý.

3. Đơn vị có trách nhiệm xây dựng quy trình 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 chuyên trách về công nghệ thông tin thực hiện quản lý, vận hành và định kỳ kiểm tra, sửa chữa, bảo trì thiết bị.

Điều 7. Bảo đảm an toàn thông tin khi sử dụng máy tính

1. Cá nhân sử dụng máy tính để xử lý công việc tuân thủ các quy định sau:

a, Chỉ cài đặt phần mềm hợp lệ (phần mềm có bản quyền thương mại; phần mềm nội bộ được đầu tư hoặc phần mềm mã nguồn mở có nguồn gốc rõ ràng); thường xuyên cập nhật phần mềm và hệ điều hành.

b, Cài đặt phần mềm xử lý phần mềm độc hại và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm; thực hiện kiểm tra, rà quét phần mềm độc hại khi sao chép, mở các tập tin hoặc trước khi kết nối các thiết bị lưu trữ dữ liệu di động với máy tính của mình.

c, Khi phát hiện ra 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 công nghệ thông tin để được xử lý kịp thời.

d, 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; sử dụng những trình duyệt an toàn; không truy nhập, mở các trang tin, thư điện tử không rõ nguồn gốc; không sử dụng tính năng lưu mật khẩu tự động hoặc đăng nhập tự động.

e, Có trách nhiệm bảo mật tài khoản truy nhập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác. Đặt mật khẩu với độ an toàn cao và thường xuyên thay đổi mật khẩu; đăng xuất tài khoản khi không sử dụng; thường xuyên xóa các biểu mẫu, mật khẩu, bộ nhớ cache và cookie trong trình duyệt trên máy tính.

f, Đặt mật khẩu khóa máy tính khi rời khỏi phòng làm việc; tắt máy tính khi rời khỏi Học viện.

2. Các đơn vị phổ biến quy chế, quy định về bảo đảm an toàn thông tin khi sử dụng máy tính đến tất cả các cá nhân trong đơn vị mình để tuân thủ thực hiện.

3. Tài khoản truy nhập:

a, Cá nhân sử dụng hệ thống thông tin được cấp và sử dụng tài khoản truy nhập 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, thôi học (với sinh viên, học viên), trong vòng không quá 5 ngày đơn vị quản lý cá nhân đó phải thông báo đơn vị chủ quản hệ thống thông tin để điều chỉnh, thu hồi, hủy bỏ các quyền sử dụng đối với hệ thống thông tin. Với email sẽ được duy trì trong vòng 15 ngày, những trường hợp đặc biệt sẽ do Giám đốc Học viện quyết định.

c, Tài khoản quản trị hệ thống phải tách biệt với tài khoản truy nhập của người sử dụng thông thường. Tài khoản quản trị hệ thống phải được giao đích danh cá nhân.

Điều 8. Bảo đảm an toàn thông tin đối với mạng máy tính

Hệ thống mạng nội bộ (LAN) phải được thiết kế phân vùng theo chức năng cơ bản, 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.

Căn cứ điều kiện, yêu cầu thực tế về bảo mật dữ liệu, Bộ phận CNTT triển khai xây dựng mô hình, giải pháp an toàn bảo mật, bao gồm các biện pháp kỹ thuật sau đây:

a, Kiểm soát truy cập từ bên ngoài mạng.

b, Kiểm soát truy cập từ bên trong mạng (quản lý thiết bị đầu cuối, máy tính người sử dụng kết nối vào hệ thống mạng; giám sát, phát hiện và ngăn chặn truy nhập từ bên trong mạng đến các địa chỉ internet bị cấm truy nhập).

c, Phòng, chống xâm nhập và phần mềm độc hại, bảo vệ các vùng mạng máy chủ và vùng mạng nội bộ.

d, Cấu hình chức năng xác thực trên các thiết bị kết nối mạng để các thực người sử dụng quản trị thiết bị trực tiếp hoặc từ xa.

e, Mạng không dây phải có cơ chế bảo toàn tính toàn vẹn và bí mật của thông tin được truyền đưa trên môi trường mạng, có hướng dẫn bảo đảm an toàn thông tin dành cho các thiết bị đầu cuối khi kết nối vào mạng; được thiết lập các tham

số: tên, nhận dạng dịch vụ, mật khẩu, cấp phép truy nhập đối với địa chỉ vật lý, mã hóa dữ liệu. Thường xuyên thay đổi mật khẩu. Các điểm truy nhập không dây phải được bảo vệ, tránh bị tiếp cận trái phép.

f, Các đơn vị, cá nhân không được tiết lộ phương thức (tên đăng ký, mật khẩu...) để truy nhập vào hệ thống mạng của Học viện; không được tìm cách truy nhập dưới bất kỳ hình thức nào vào hệ thống mạng của Học viện.

g, Có hệ thống tường lửa (firewall) và hệ thống bảo vệ kiểm soát truy nhập internet, đáp ứng nhu cầu kết nối đồng thời, quản lý luồng dữ liệu vào, ra và có khả năng bảo vệ hệ thống trước các tấn công từ chối dịch vụ.

h, Lọc bỏ, không cho phép truy nhập các trang tin có nghi ngờ chứa mã độc

Điều 9. Bảo đảm an toàn thông tin phần mềm ứng dụng

Các đơn vị vận hành, sử dụng phần mềm phải đáp ứng các yêu cầu sau:

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

b, Cấu hình phần mềm ứng dụng để xác thực người dùng; giới hạn số lần đăng nhập sai liên tiếp, 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 với người sử dụng/nhóm người sử dụng có chức năng, yêu cầu nghiệp vụ khác nhau.

d, Chỉ cho phép sử dụng các giao thức mạng có hỗ trợ chức năng mã hóa thông tin hoặc tương đương khi truy nhập, quản trị phần mềm, ứng dụng từ xa thông qua môi trường mạng; hạn chế truy nhập tới mã nguồn của phần mềm và phải đặt mã nguồn trong môi trường an toàn do cán bộ quản lý phần mềm ứng dụng tại các đơn vị quản lý.

e, Ghi và lưu giữ bản ghi nhật ký hệ thống của phần mềm với những thông tin cơ bản: thời gian, địa chỉ, tài khoản, nội dung truy nhập và sử dụng phần mềm; các lỗi phát sinh trong qua trình hoạt động; thông tin đăng nhập khi quản trị.

f. Thực hiện quy trình kiểm soát việc cài đặt, cập nhật, vá lỗi bảo mật phần mềm trên máy chủ, máy tính cá nhân, thiết bị kết nối mạng đang hoạt động trong mạng nội bộ của Học viện.

g. Kiểm tra phát hiện và khắc phục điểm yếu của ứng dụng trước khi đưa vào sử dụng và trong quá trình sử dụng.

Điều 10. Bảo đảm an toàn thông tin dữ liệu

1. Các đơn vị quản lý, vận hành, sử dụng phần mềm phải có các phương án bảo vệ thông tin, dữ liệu như sau:

a, Thiết lập phương án bảo đảm tính bí mật, nguyên vẹn và khả dụng của thông tin, dữ liệu; giám sát, cảnh báo khi có thay đổi hoặc phát hiện, ngăn chặn các tác động truy nhập, gửi, nhận dữ liệu trái phép.

b, Mã hóa thông tin, dữ liệu khi lưu trữ trên hệ thống lưu trữ/thiết bị lưu trữ dữ liệu; thiết lập phân vùng lưu trữ mã hóa, chỉ cho phép các nhân có quyền, trách nhiệm truy nhập, lưu trữ dữ liệu trên phân vùng mã hóa.

c, 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 gắn 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.

2. Các đơn vị phải thường xuyên kiểm tra, giám sát 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.

3. Đối với hoạt động trao đổi thông tin, dữ liệu với bên ngoài, các 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; yêu cầu bên ngoài đáp ứng các thỏa thuận kết nối, bảo vệ thông tin phù hợp với quy định về bảo đảm an toàn thông tin của Học viện; thiết lập chức năng phát hiện dữ liệu đính kèm có phần mềm độc hại, mã hóa thông tin, dữ liệu trước khi truyền đưa, trao đổi trên môi trường mạng theo quy định của pháp luật.

4. 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 cơ chế xác thực mạnh, sử dụng các giao thức truyền thông an toàn.

Điều 11. Bảo đảm an toàn thông tin khi tiếp nhận, phát triển, vận hành và bảo trì hệ thống thông tin

1. Khi tiếp nhận, phát triển, nâng cấp, bảo trì hệ thống thông tin đơn vị quản lý hệ thống mạng phải tiến hành phân tích, xác định các 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 bên cung cấp, thi công, các cá nhân liên quan thực hiện.

Một số yêu cầu như sau:

a, Có phương án bảo đảm an toàn thông tin;

b, Chỉ tiếp nhận và đưa vào vận hành hệ thống thông tin sau khi đã thực hiện nghiệm thu và kiểm thử hệ thống;

c, Hệ thống thông tin được tiếp nhận phải đi kèm:

- Tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin;

- Tài liệu mô tả các thành phần của hệ thống thông tin, gồm: Các vùng mạng chức năng, hệ thống thiết bị mạng, thiết bị bảo mật; hệ thống máy chủ hệ thống; hệ thống máy chủ ứng dụng; dịch vụ và các thành phần khác trong hệ thống thông tin.

d, Xem xét tính tương thích các phần mềm, ứng dụng hiện có, bảo đảm hoạt động ổn định, an toàn trước khi thay đổi hoặc nâng cấp hệ điều hành lên phiên bản mới; kiểm soát chặt chẽ việc nâng cấp, mở rộng phần mềm, ứng dụng trong hệ thống. Việc bổ sung các thiết bị vào hệ thống thông tin cần có kế hoạch, quy trình bảo đảm việc tiếp nhận không làm gián đoạn hoạt động của hệ thống đang vận hành.

2. Trong qua trình vận hành hệ thống thông tin, đơn vị chủ quản hệ thống cần thực hiện:

a, Đánh giá, phân loại hệ thống thông tin; triển khai phương án đảm bảo 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.

b, Thường xuyên kiểm tra, giám sát việc tuân thủ các quy định về an toàn thông tin, cập nhật đầy đủ các lỗ hổng bảo mật, áp dụng cơ chế sao lưu dự phòng, bảo đảm an toàn truy nhập, đăng nhập hệ thống.

c, Giám sát an toàn hệ thống thông tin, cảnh báo hành vi xâm phạm an toàn thông tin hoặc hành vi có khả năng gây ra sự cố an toàn thông tin đối với hệ thống thông tin; tiến hành phân tích yếu tố then chốt ảnh hưởng tới trạng thái an toàn thông tin; đề xuất thay đổi biện pháp kỹ thuật.

d, Giám sát hiệu năng hệ thống và thực hiện các biện pháp bảo trì cần thiết để bảo đảm khả năng xử lý và tính sẵn sàng của hệ thống thông tin theo yêu cầu.

e, Tuân thủ quy trình vận hành, quy trình xử lý sự cố; ghi đầy đủ thông tin trong các bản ghi hệ thống và lưu trữ nhật ký trong khoảng thời gian nhất định, để phục vụ việc quản lý, kiểm soát thông tin.

3. Đối tác phát triển phần mềm, ứng dụng có trách nhiệm đảm bảo đảm an toàn thông tin cho công tác phát triển, vận hành, bảo hành, bảo trì phần mềm, tránh lộ lọt mã nguồn và dữ liệu, tài liệu thiết kế, quản trị hệ thống mà đối tác đang xử lý bên ngoài.

4. Các biện pháp kỹ thuật đảm bảo an toàn thông tin cho trang cổng thông tin điện tử:

a, Xác định cấu trúc thiết kế trang/cổng thông tin điện tử: quản lý toàn bộ các phiên bản của mã nguồn của phần mềm, ứng dụng trang/cổng thông tin điện tử; phối hợp với đơn vị quản lý máy chủ tổ chức mô hình trang/cổng thông tin điện tử hợp lý tránh khả năng bị tấn công; yêu cầu đơn vị cung cấp dịch vụ hosting phải cài đặt hệ thống phòng vệ như tường lửa, thiết bị phát hiện, phòng, chống xâm nhập ở mức ứng dụng web.

b, Vận hành phần mềm, ứng dụng trang/cổng thông tin điện tử: các trang/công thông tin điện tử khi đưa vào sử dụng hoặc khi bổ sung thêm các chức

năng cần đánh giá kiểm định nhằm tránh được các lỗi bảo mật thường xảy ra trên ứng dụng web.

c. Thiết lập và cấu hình cơ sở dữ liệu của trang/cổng thông tin điện tử:

- Luôn cập nhật bản vá lỗi mới nhất cho hệ quản trị cơ sở dữ liệu; sử dụng công cụ đánh giá, tìm kiếm lỗ hổng trên máy chủ cơ sở dữ liệu.

- Gỡ bỏ các cơ sở dữ liệu không còn sử dụng.

- Có cơ chế sao lưu dữ liệu tự động theo định kỳ tối thiểu 1 lần/ ngày, nên sao lưu vào thiết bị lưu trữ hoặc máy chủ khác với máy chủ cơ sở dữ liệu.

d, Phối hợp với đơn vị quản lý máy chủ xây dựng phương án phục hồi trang/cổng thông tin điện tử trong trường hợp bị đánh sập, trong đó chú ý nhất mỗi tháng thực hiện việc sao lưu toàn bộ nội dung trang/cổng thông tin điện tử 01 lần bao gồm mã nguồn, cơ sở dữ liệu để đảm bảo khi có sự cố có thể khắc phục trong thời gian sớm nhất.

Điều 12: Kiểm tra, khắc phục sự cố an toàn thông tin

1. Đối với cá nhân

a) Thông báo kịp thời cho cán bộ công nghệ thông tin khi phát hiện các sự cố gây mất an toàn thông tin trong hệ thống.

b) Xử lý khẩn cấp: Khi phát hiện hệ thống gặp sự cố, thông qua các dấu hiệu khác thường như: Hệ thống máy tính hoạt động chậm khác thường, nội dung bị thay đổi,... cần báo ngay cho cán công nghệ thông tin để có hướng xử lý kịp thời.

2. Đối với bộ phận Công nghệ thông tin.

Hướng dẫn người dùng nắm được những nguyên tắc hoạt động cơ bản nhất của máy tính và một số giải pháp khắc phục sự cố đơn giản mà hệ thống CNTT hay gặp phải; trong trường hợp sự cố xảy ra ngoài khả năng giải quyết, kịp thời thông tin ngay với bộ CNTT đồng thời phối hợp với các đơn vị có liên quan để cùng phối hợp khắc phục.

Thường xuyên theo dõi, tổng hợp, nắm tình hình, tham mưu các văn bản chỉ đạo về AT-ANTT.

Tham mưu cho Ban giám đốc các phương án nâng cấp và xử lý đảm bảo hệ thống CNTT luôn hoạt động trong trạng thái ổn định và an toàn.

CHƯƠNG III
TỔ CHỨC THỰC HIỆN

Điều 13. Trách nhiệm của đơn vị

1. Chỉ đạo, bảo đảm việc tuân thủ các quy định của Quy chế này trong phạm vi tổ chức, quyền hạn của mình.

2. Căn cứ Quy chế này và nhu cầu thực tế của đơn vị, xây dựng hoặc rà soát sửa đổi phương án quản lý an toàn thông tin đang áp dụng cho phù hợp.

3. Tuyên truyền, phổ biến nội dung Quy chế này tới từng cá nhân trong đơn vị: nâng cao nhận thức cho các cá nhân về nguy cơ mất an toàn thông tin.

4. Phối hợp, cung cấp thông tin và tạo điều kiện cho bộ phận công nghệ thông tin và các đối tác, vận hành hệ thống thông tin và an toàn thông tin của Học viện triển khai công tác kiểm tra khắc phục sự cố xảy ra một cách kịp thời, nhanh chóng và đạt hiệu quả.

Điều 14. Trách nhiệm của các cá nhân

1. Cá nhân phụ trách an toàn thông tin có trách nhiệm:

a, Tham mưu cho Ban giám đốc, lãnh đạo đơn vị ban hành các quy định, quy trình nội bộ và chịu trách nhiệm triển khai các giải pháp kỹ thuật bảo đảm an toàn thông tin tại Học viện, đơn vị theo quy chế này.

b, Thực hiện việc giám sát, đánh giá, báo cáo Ban giám đốc, lãnh đạo đơn vị các rủi ro mất an toàn thông tin.

c, Phối hợp với các cá nhân, đơn vị có liên quan trong việc kiểm tra, phát hiện và khắc phục các sự cố mất an toàn thông tin.

2. Cá nhân là người sử dụng có trách nhiệm:

a, Chấp hành nghiêm túc các quy định về an toàn thông tin của Học viện; nâng cao ý thức cảnh giác và trách nhiệm bảo đảm an toàn thông tin trong phạm vi trách nhiệm và quyền hạn được giao.

b, Tự quản lý, bảo quản thiết bị mà mình được giao sử dụng. Khi phát hiện sự cố phải báo ngay với cấp trên và bộ phận chuyên trách về CNTT để kịp thời ngăn chặn, xử lý.

c, Tích cực tham gia các chương trình đào tạo, bồi dưỡng về an toàn thông tin do các bộ phận chuyên môn tổ chức.

Điều 15. Điều khoản thi hành

Trong qua trình thực hiện quy chế này, nếu có vướng mắc, các đơn vị, cá nhân phản ánh về Tổ quản trị và Bảo mật hệ thống của Học viện để tổng hợp, báo cáo Ban giám đốc xem xét sửa đổi, bổ sung Quy chế cho phù hợp.