BỘ TƯ PHÁP
TRƯỜNG ĐẠI HỌC LUẬT HÀ NỘI

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

Số: 2580 /QĐ-ĐHLHN

Hà Nội, ngày 05 tháng 7 năm 2022

QUYẾT ĐỊNH
Ban hành Quy chế bảo đảm an toàn, an ninh thông tin mạng tại Trường Đại học Luật Hà Nội

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Luật Công nghệ thông tin ngày 29 tháng 6 năm 2006;

Căn cứ Luật Viễn thông ngày 23 tháng 11 năm 2009;

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;

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 Quyết định số 1622/QĐ-TTg ngày 25 tháng 10 năm 2017 của Thủ tướng Chính phủ về việc phê duyệt Đề án đẩy mạnh hoạt động của mạng lưới ứng cứu sự cố, tăng cường năng lực cho cán bộ, bộ phận chuyên trách ứng cứu sự cố an toàn thông tin mạng trên toàn quốc đến 2020, định hướng đến 2025;

Căn cứ Thông tư số 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 của Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin;

Căn cứ Quyết định số 405/CP ngày 10/11/1979 của Hội đồng Chính phủ về việc thành lập Trường Đại học Pháp lý Hà Nội (nay là Trường Đại học Luật Hà Nội);

Căn cứ Quyết định số 868/QĐ-BTP ngày 07/5/2015 của Bộ trưởng Bộ Tư pháp quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Trường Đại học Luật Hà Nội;

Căn cứ Nghị quyết số 3776/NQ-HĐTĐHLHN ngày 23 tháng 10 năm 2020 của Hội đồng trường Đại học Luật Hà Nội ban hành Quy chế tổ chức và hoạt động của Trường Đại học Luật Hà Nội;

Xét 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, an ninh thông tin mạng Trường Đại học Luật Hà Nội".

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

Điều 3. Giám đốc Trung tâm Công nghệ thông tin, lãnh đạo các đơn vị, và các tổ chức, cá nhân liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Hội đồng Trường (để chỉ đạo t/h)
- Các Phó Hiệu trưởng (để chỉ đạo t/h);
- Trưởng các đơn vị (để t/h);
- Lưu: VT, TTCNTT.

HIỆU TRƯỞNG

TRƯỜNG ĐẠI HỌC LUẬT HÀ NỘI

Đoàn Trung Kiên

BỘ TƯ PHÁP
TRƯỜNG ĐẠI HỌC LUẬT HÀ NỘI

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

QUY CHẾ
Bảo đảm an toàn, an ninh thông tin mạng tại Trường Đại học Luật Hà Nội

(Ban hành kèm theo Quyết định số 2580/QĐ-ĐHLHN ngày 05 tháng 7 năm 2022 của Hiệu trưởng Trường Đại học Luật Hà Nội)

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, an ninh thông tin mạng trong các hoạt động của Trường Đại học Luật Hà Nội và các đơn vị thuộc Trường.

2. Đối tượng áp dụng:

a) Các đơn vị thuộc Trường Đại học Luật Hà Nội (sau đây gọi là đơn vị thuộc Trường) và viên chức, người lao động thuộc các đơn vị thuộc Trường.

b) Cơ quan, tổ chức, cá nhân có kết nối vào hệ thống mạng của Trường Đại học Luật Hà Nội.

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

Điều 2. Giải thích từ ngữ

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 thông tin 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. *Bảo đảm an toàn thông tin mức vật lý* là việc bảo vệ hệ thống 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 của hệ thống;

4. *Không gian mạng* là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng internet, hệ thống máy tính, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian;

5. *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;

6. *Trang thông tin điện tử* là trang thông tin hoặc tập hợp trang thông tin trên không gian mạng phục vụ cho việc cung cấp, trao đổi thông tin;

7. *Cổng thông tin điện tử* là điểm truy nhập duy nhất của cơ quan, đơn vị trên không gian 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;

8. *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.

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

1. Bảo đảm an toàn, an ninh thông tin mạng 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 Điều 4 Luật An toàn thông tin mạng và Điều 4 Nghị định số 85/2016/NĐ-CP.

2. Các đơn vị thuộc Trường có trách nhiệm bảo đảm an toàn, an ninh thông tin mạng của đơn vị mình; 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.

3. Viên chức và người lao động trong các đơn vị thuộc Trường 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 Trường Đại học Luật Hà Nội.

4. Thông tin thuộc bí mật công tác của Trường, thông tin thuộc Danh mục bí mật nhà nước phải được bảo vệ theo quy định của Nhà nước, quy định của Bộ Tư pháp về công tác bảo vệ bí mật nhà nước và các nội dung tương ứng trong Quy chế này.

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.

a) Ngăn chặn việc truyền tải thông tin trên mạng, can thiệp, truy nhập, gây nguy hại, xóa, thay đổi, sao chép và làm sai lệch thông tin trên mạng trái pháp luật.

b) Gây ảnh hưởng, cản trở trái pháp luật tới hoạt động bình thường của hệ thống thông tin hoặc tới khả năng truy nhập hệ thống thông tin của người sử dụng.

c) Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của biện pháp bảo vệ an toàn thông tin mạng của hệ thống thông tin; tấn công, chiếm quyền điều khiển, phá hoại hệ thống thông tin.

d) Phát tán thư rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo.

e) Thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác; lợi dụng sơ hở, điểm yếu của hệ thống thông tin để thu thập, khai thác thông tin cá nhân.

f) Xâm nhập trái pháp luật bí mật mật mã và thông tin đã mã hóa hợp pháp của cơ quan, tổ chức, cá nhân; tiết lộ thông tin về sản phẩm mật mã dân sự, thông tin về khách hàng sử dụng hợp pháp sản phẩm mật mã dân sự; sử dụng, kinh doanh các sản phẩm mật mã dân sự không rõ nguồn gốc.

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; 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...).

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. Tạo ra, cài đặt, phát tán phần mềm độc hại.

5. Bẻ khóa, lấy cắp thông tin, sử dụng mật khẩu, khóa mật mã và thông tin của cơ quan, cá nhân khác trên không gian mạng.

6. Các hành vi khác làm mất an toàn, an ninh thông tin mạng của Trường, cơ quan, tổ chức, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên không gian mạng.

CHƯƠNG II
NGUYÊN TẮC BẢO ĐẢM AN TOÀN, AN NINH THÔNG TIN MẠNG

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

1. Giao, gắn trách nhiệm cho cá nhân hoặc tập thể quản lý, sử dụng trang thiết bị công nghệ thông tin.

2. Quy định các quy tắc sử dụng, giữ gìn bảo vệ trang thiết bị công nghệ thông tin trong các trường hợp như: mang ra khỏi cơ quan, trang thiết bị công nghệ thông tin liên quan đến dữ liệu nhạy cảm, cài đặt và cấu hình.

Điều 6. Bảo đảm an toàn thông tin khi sử dụng máy tính

1. Cá nhân chỉ 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 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.

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

Điều 7. Lưu trữ và trao đổi thông tin

1. Việc lưu trữ và trao đổi thông tin phải tuân thủ các quy định của pháp luật về bưu chính, viễn thông và công nghệ thông tin.

2. Các thông tin bị cấm lưu trữ, trao đổi trên mạng và đưa lên Cổng thông tin của Trường:

a) Thông tin chưa được cấp có thẩm quyền cho phép công bố;

b) Thông tin thuộc bí mật công tác theo các quy định của Trường;

c) Thông tin thuộc danh mục thông tin mật do pháp luật quy định;

d) Thông tin và các dịch vụ bất hợp pháp, độc hại.

Điều 8. Phương án bảo đảm an toàn hệ thống thông tin

1. Nội dung phương án bảo đảm an toàn hệ thống thông tin bao gồm:

Các nội dung phải tuân thủ quy định của Nhà nước:

- Quản lý an toàn thông tin mạng: Chính sách chung; tổ chức, nhân sự; quản lý thiết kế, xây dựng; quản lý vận hành; kiểm tra, đánh giá và quản lý rủi ro.

- Phương án kỹ thuật: An toàn hạ tầng mạng; an toàn máy chủ; an toàn ứng dụng và an toàn dữ liệu; an toàn vật lý cho Phòng máy chủ.

- Phần dùng chung cho các hệ thống bao gồm: quản lý an toàn thông tin mạng; an toàn hạ tầng mạng; an toàn vật lý Phòng máy chủ; an toàn kết nối Internet; an toàn trong trao đổi thông tin với các tổ chức, cá nhân ngoài Trường; an toàn tài khoản công nghệ thông tin; An toàn máy tính phục vụ công việc; an toàn vật lý các thiết bị công nghệ thông tin.

Điều 9. Triển khai phương án bảo đảm an toàn hệ thống thông tin

1. Hệ thống mạng Nhà trường phải được trang bị hệ thống trang thiết bị để sao lưu dữ liệu thường xuyên, liên tục quản lý, giám sát, kiểm soát, duy trì mạng, nhằm phát hiện ngăn chặn các truy cập trái phép của người sử dụng, tin tặc tấn công mạng và triển khai cơ chế phòng, chống virus tại các máy chủ, máy trạm trong mạng.

2. Trung tâm Công nghệ thông tin phối hợp cùng Phòng Quản trị tổ chức triển khai phương án bảo đảm An toàn hệ thống thông tin trong Trường.

CHƯƠNG III
TRÁCH NHIỆM CỦA CÁC ĐƠN VỊ, CÁ NHÂN LIÊN QUAN

Điều 10. Trách nhiệm của đơn vị, cá nhân đối với công tác an ninh, an toàn thông tin mạng

1. Viên chức, người lao động, người học của Nhà trường thuộc đối tượng áp dụng của Quy chế có trách nhiệm tuân thủ Quy chế; nâng cao trách nhiệm bảo đảm an ninh, an ninh thông tin, thông báo các vấn đề bất thường liên quan tới an toàn thông tin cho đơn vị; Sử dụng các dịch vụ an toàn mạng, bảo mật thông tin, không mở thư lạ, thư rác đính kèm liên kết để tránh virus; không vào các trang thông tin điện tử không có nguồn gốc xuất xứ rõ ràng.

2. Cơ quan, tổ chức, cá nhân ngoài Trường có liên quan: Tuân thủ Quy chế này, quy định công tác bảo vệ bí mật nhà nước của ngành Tư pháp, các cam kết, thỏa thuận với Nhà trường để đảm bảo an toàn thông tin khi cung cấp dịch vụ công nghệ thông tin và thực hiện các hoạt động trao đổi thông tin với cá đơn vị thuộc Trường.

3. Lãnh đạo các đơn vị thuộc Trường có trách nhiệm: phổ biến tới từng viên chức, người lao động của đơn vị; thường xuyên kiểm tra việc thực hiện Quy chế này tại đơn vị.

4.Viên chức, người lao động của Trường Đại học Luật Hà Nội 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 Trường.

Điều 11. Trách nhiệm của Trung tâm Công nghệ thông tin

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

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

3. Chủ trì và phối hợp với các đơn vị có liên quan triển khai thực hiện Quy chế này tại Trường Đại học Luật Hà Nội.

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

Điều 12. Trách nhiệm của các đơn vị thuộc Trường và các tổ chức chính trị - xã hội của Trường

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

2. Tổ chức triển khai thực hiện Quy chế này tại đơn vị.

3. Thực hiện các báo cáo theo quy định, gửi Trung tâm Công nghệ thông tin tổng hợp, báo cáo lãnh đạo Trường.

4. Xây dựng, 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.

5. Phối hợp với Trung tâm 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 Trường và các hệ thống thông tin do đơn vị quản lý, vận hành.

CHƯƠNG IV
TỔ CHỨC THỰC HIỆN

Điều 13. Kinh phí thực hiện

1. Kinh phí bảo đảm an toàn, an ninh thông tin mạng được cấp từ nguồn chi thường xuyên dự toán hàng năm của Trường Đại học Luật Hà Nội.

2. Căn cứ vào kế hoạch hàng năm, các đơn vị liên quan có trách nhiệm xây dựng kế hoạch, đề xuất dự toán cho các hoạt động bảo đảm an toàn, an ninh thông tin mạng gửi Trung tâm Công nghệ thông tin để tổng hợp, gửi Ban Giám hiệu phê duyệt.

Điều 14. Trách nhiệm thi hành

1. Thủ trưởng các đơn vị trực thuộc Trường có trách nhiệm phổ biến, quán triệt đến toàn bộ viên chức, người lao động trong đơn vị thực hiện các quy định của Quy chế này.

2. 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 Hiệu trưởng xem xét, sửa đổi, bổ sung quy chế./.