BỘ TÀI CHÍNH
TRƯỜNG ĐẠI HỌC
TÀI CHÍNH – QUẢN TRỊ KINH DOANH

Số: 676 /QĐ-ĐHTCQTKD

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

Hưng Yên, ngày 09 tháng 11 năm 2018

QUYẾT ĐỊNH

Ban hành quy chế đảm bảo an toàn, an ninh thông tin mạng trường Đại học Tài chính – Quản trị kinh doanh

HIỆU TRƯỞNG TRƯỜNG ĐẠI HỌC TÀI CHÍNH – QUẢN TRỊ KINH DOANH

Căn cứ Luật An toàn thông tin mạng năm 2015;

Căn cứ 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;

Căn cứ Quyết định số 632/QĐ-TTg ngày 10/5/2017 của Thủ tướng Chính phủ ban hành Danh mục lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng và hệ thống thông tin quan trọng quốc gia;

Căn cứ Quyết định số 1622/QĐ-TTg ngày 25/10/2017 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 15/11/2017 của Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin;

Căn cứ Quyết định số 201/QĐ-BTC ngày 12/02/2018 của Bộ Tài chính về ban hành quy chế an toàn thông tin mạng Bộ Tài chính;

Xét đề nghị của Giám đốc Trung tâm Thông tin – Thư viện,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này "Quy chế đảm bảo an toàn, an ninh thông tin mạng Trường Đại học Tài chính – Quản trị kinh doanh"

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

Điều 3. Giám đốc Trung tâm Thông tin – Thư viện, lãnh đạo các đơn vị, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- BGH
- Các đơn vị;
- website nhà trường;
- Lưu: VT, Trung tâm TTTV.

HIỆU TRƯỞNG

BỘ TÀI CHÍNH TRƯỜNG ĐẠI HỌC TÀI CHÍNH QUẢN TRỊ KINH DOANH

TS. Nguyễn Trọng Nghĩa

BỘ TÀI CHÍNH
TRƯỜNG ĐẠI HỌC
TÀI CHÍNH – QUẢN TRỊ KINH DOANH

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

QUY CHẾ

Đảm bảo an toàn, an ninh thông tin mạng
trường Đại học Tài chính – Quản trị kinh doanh
(Kèm theo Quyết định số 676 /QĐ-ĐHTCQTKD ngày 09 tháng 11 năm 2018 của Hiệu trưởng Đại học Tài chính – Quản trị kinh doanh)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh: Quy chế này triển khai áp dụng Luật An toàn thông tin mạng, văn bản quy định, tiêu chuẩn liên quan và các biện pháp nhằm bảo đảm an toàn thông tin và các hệ thống thông tin của trường Đại học Tài chính – Quản trị kinh doanh.

2. Đối tượng áp dụng:

a) Cơ quan, tổ chức, cá nhân có kết nối vào mạng máy tính của trường Đại học Tài chính – Quản trị kinh doanh.

b) 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 Đại học Tài chính – Quản trị kinh doanh.

Điều 2. Giải thích từ ngữ sử dụng trong Quy chế

1. "An toàn thông tin mạng": Sự bảo vệ thông tin số và hệ thống thông tin khỏi 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. "Kết nối Internet": Kết nối mạng tới hệ thống mạng Internet nhằm cung cấp khả năng truy cập Internet hoặc cung cấp thông tin, dịch vụ ra Internet.

3. "Mạng nội bộ": Mạng máy tính trong phạm vi trụ sở của nhà trường

4. "Mạng của ngành Tài chính": Từ chỉ chung "mạng nội bộ", "hạ tầng truyền thông thống nhất ngành Tài chính".

5. "Phòng chống xâm nhập": phát hiện, ngăn chặn các hoạt động vào, ra trên hệ thống thông tin được bảo vệ có dấu hiệu gây hại hoặc vi phạm chính sách an toàn mạng.

6. "Truy cập Internet": Việc tiếp cận, khai thác, sử dụng thông tin, tài liệu, ứng dụng, dịch vụ trên Internet.

Điều 3. Nguyên tắc bảo đảm an toàn thông tin mạng tại trường Đại học Tài chính – Quản trị kinh doanh

1. Cán bộ, giảng viên, nhân viên, lãnh đạo các Phòng, Khoa, Trung tâm thuộc Trường có trách nhiệm bảo đảm an toàn thông tin và hệ thống thông tin trong phạm vi xử lý công việc của mình theo quy định của Nhà nước, trong lĩnh vực bảo đảm an toàn thông tin mạng.

2. Bảo đảm an toàn thông tin mạng phải được thực hiện tại tất cả các công đoạn liên quan đến thông tin và hệ thống thông tin.

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

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.

2. Tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập 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.

Chương II

BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN

Điều 5. Các loại thông tin trên mạng Nhà trường

1. Các cơ sở dữ liệu phục vụ công tác quản lý, điều hành của nhà trường và các đơn vị trong trường.

2. Cổng thông tin điện tử của Nhà trường.

3. Thông tin trao đổi giữa các đơn vị trong trường.

4. Thông tin trao đổi giữa Người sử dụng với nhau.

Điều 6. Các dịch vụ trên mạng

1. Các dịch vụ được cấp từ các hệ thống ứng dụng tin học phục vụ công tác quản lý, điều hành của Nhà trường và các đơn vị trực thuộc (Hệ thống thư điện tử, Hệ thống quản lý văn bản, Cơ sở dữ liệu chuyên ngành.)

2. Các dịch vụ từ Website của Nhà trường (Tin tức hoạt động; tin chỉ đạo điều hành; Các thông báo; Các quyết định; hệ thống văn bản; hệ thống danh bạ điện tử….v.v)

3. Các dịch vụ chia sẻ tài nguyên trên mạng như: Truyền file, gửi mail, dùng chung ổ cứng, dùng chung máy in…v.v

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 Website của Nhà trường:

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

b, Thông tin thuộc danh mục thông tin mật do pháp luật quy định;

c, Thông tin cá nhân như: Tài sản cá nhân, đời tư, các sản phẩm nghiên cứu khoa học công nghệ mà người sở hữu chưa cho phép công bố rộng rãi.

d, Thông tin và các dịch vụ bất hợp pháp, độc hại như:

- Làm ảnh hưởng đến an ninh quốc gia;

- Xuyên tạc, tuyên truyền chống đối các chủ trương chính sách của Đảng và Nhà nước, phá hoại khối đại đoàn kết dân tộc;

- Có nội dung kích động bạo lực, tuyên truyền chiến tranh xâm lược, gây hận thù giữa các dân tộc và nhân dân các nước, truyền bá tư tưởng phản động;

- Làm ảnh hưởng đến đời tư công dân: các thông tin quấy rối cá nhân, xúc phạm danh dự, vu khống, xúc phạm đến nhân phẩm công dân;

- Làm ảnh hưởng đến an ninh kinh tế: thông tin lừa đảo, thông tin bí mật kinh tế;

- Vi phạm quyền sở hữu trí tuệ: sử dụng và truyền bá trái phép các sản phẩm có bản quyền, phần mềm tin học, âm nhạc, tác phẩm văn học, tác phẩm nghệ thuật;

- Làm ảnh hưởng đến an toàn thông tin: các ứng dụng có tính chất phá hoại như virus tin học, lấy cắp thông tin, phá hoại cơ sở dữ liệu, làm tê liệt mạng máy tính;

- Có ảnh hưởng xấu đến văn hoá xã hội: xuyên tạc lịch sử, phủ nhận các thành quả cách mạng, xúc phạm các vĩ nhân và các anh hùng dân tộc, phao tin đồn nhảm ảnh hưởng đến uy tín của Quốc gia;

- Trái với thuần phong mỹ tục như: các thông tin khiêu dâm, đồi trụy, tệ nạn xã hội, nghiện hút, cờ bạc, mê tín dị đoan, sử dụng các từ ngữ thô tục, nội dung không lành mạnh, thiếu văn hoá, các thông tin ảnh hưởng đến quyền tự do tín ngưỡng của nhân dân.

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

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

a) 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 Trung tâm dữ liệu/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 Trung tâm dữ liệu/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.

Trong đó, phương án quản lý an toàn thông tin mạng; an toàn hạ tầng mạng; an toàn vật lý Trung tâm dữ liệu/phòng máy chủ phải đáp ứng yêu cầu tương ứng với cấp độ cao nhất trong số các cấp độ được xác định cho các hệ thống thông tin do đơn vị quản lý và tối thiểu đáp ứng yêu cầu:

b) Phần áp dụng cho từng hệ thống thông tin cụ thể: an toàn máy chủ, an toàn ứng dụng, an toàn cơ sở dữ liệu, an toàn tài khoản công nghệ thông tin và các nội dung liên quan khác.

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 kỹ thuật hiện đại để 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 phải được triển khai cơ chế chống virus, thư rác cho những hệ thống xung yếu hiện hữu (web server, mail server ….) tại các máy trạm, máy chủ trong mạng; tổ chức sử dụng cơ chế chống virus, thư rác để phát hiện và loại trừ những đoạn mã độc hại (virus, trojan, worms…) có khả năng khai thác lỗ hổng của hệ thống thông tin, được truyền tải bởi thư điện tử, tập đính kèm từ Internet, thiết bị lưu trữ tháo lắp (USB, ổ cứng ngoài); đồng thời thường xuyên cập nhật cơ chế chống virus, thư rác.

2. Trung tâm Thông tin Thư viện phối hợp cùng Phòng Quản trị thiết bị tổ chức triển khai phương án bảo đảm An toàn hệ thống thông tin sau khi hồ sơ đề xuất cấp độ hoặc phương án bảo đảm an toàn hệ thống được phê duyệt.

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

1. Các đơn vị vận hành hệ thống thông tin

a) Thực hiện trách nhiệm của đơn vị vận hành hệ thống thông tin theo quy định tại Quy chế này và các nhiệm vụ do Hiệu trưởng phân công.

b) Chỉ đạo, phân công các bộ phận kỹ thuật thuộc đơn vị (quản lý ứng dụng; quản lý dữ liệu; vận hành hệ thống thông tin; triển khai và hỗ trợ kỹ thuật) triển khai công tác bảo đảm an toàn thông tin trong tất cả các công đoạn liên quan đến hệ thống thông tin.

c, Thực hiện đúng thẩm quyền việc sao chép, đưa thêm thông tin vào Hệ thống; chịu trách nhiệm pháp lý về thông tin do mình đưa vào Hệ thống.

2. Cán bộ, công chức, viên chức, nhân viên của Nhà trường thuộc đối tượng áp dụng của quy định có trách nhiệm: tuân thủ Quy chế; nâng cao trách nhiệm bảo đảm an toàn, an ninh thông tin, thông báo các vấn đề bất thường liên quan tới an toàn thông tin cho đơn vị. Thường xuyên kiểm tra và diệt virus, phối hợp với Trung tâm Thông tin - Thư viện để sử dụng các dịch vụ an toàn mạng, bảo mật thông tin mới, không mở các thư lạ, các tệp đính kèm hoặc các liên kết trong các

thư lạ để tránh virus; không vào các trang thông tin điện tử không có nguồn gốc xuất xứ rõ ràng.

3. 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 Tài chính, các cam kết, thỏa thuận với các Nhà trường về 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 các đơn vị thuộc Bộ Tài chính.

Chương III
ĐIỀU KHOẢN THI HÀNH

Điều 11. Xử lý vi phạm

Tổ chức, cá nhân có hành vi vi phạm Quy chế này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật theo trách nhiệm, xử phạt hành chính hoặc bị truy cứu trách nhiệm hình sự. Nếu gây thiệt hại thì phải bồi thường theo quy định hiện hành của pháp luật.

Điều 12. Trách nhiệm thi hành

1. Trung tâm Thông tin Thư viện có trách nhiệm hướng dẫn, theo dõi việc thực hiện Quy chế này.

2. Phòng Quản trị thiết bị có trách nhiệm phối hợp với Trung tâm Thông tin – Thư viện kiểm tra việc chấp hành Quy chế này.

3. Lãnh đạo các đơn vị trong phạm vi nhiệm vụ của mình có trách nhiệm đôn đốc và nhắc nhở nhân viên thuộc đơn vị mình thực hiện theo đúng các quy định của Quy chế này./.

HIỆU TRƯỞNG

BỘ TÀI CHÍNH
TRƯỜNG ĐẠI HỌC TÀI CHÍNH QUẢN TRỊ KINH DOANH

TS. Nguyễn Trọng Nghĩa