BỘ TÀI CHÍNH
TRƯỜNG ĐẠI HỌC
TÀI CHÍNH - MARKETING
Số: 3250/QĐ-ĐHTCM

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

Thành phố Hồ Chí Minh, ngày 06 tháng 12 năm 2023

QUYẾT ĐỊNH
Ban hành Quy chế đảm bảo an toàn thông tin mạng của Trường Đại học Tài chính - Marketing

HIỆU TRƯỞNG TRƯỜNG ĐẠI HỌC TÀI CHÍNH - MARKETING

Căn cứ Nghị định số 43/2011/NĐ-CP ngày 13/6/2011 của Chính phủ Quy chế về việc cung cấp thông tin và dịch vụ công trực tuyến trên Trang thông tin điện tử hoặc cổng thông tin điện tử của cơ quan Nhà nước;

Căn cứ Thông tư số 32/2017/TT-BTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông ban hành Quy chế về việc cung cấp dịch vụ công trực tuyến và bảo đảm khả năng truy cập thuận tiện đối với trang thông tin điện tử hoặc cổng thông tin điện tử của cơ quan nhà nước;

Căn cứ Nghị định số 27/2018/NĐ-CP ngày 01/3/2018 của Chính phủ sửa đổi, bổ sung một số điều của Nghị định số 72/2013/NĐ-CP ngày 15/7/2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng;

Căn cứ Thông tư số 06/2019/TT-BTTTT ngày 19/7/2019 của Bộ Thông tin và Truyền thông sửa đổi, bổ sung một số điều của Thông tư số 24/2015/TT-BTTTT ngày 18 tháng 8 năm 2015 của Bộ trưởng Bộ Thông tin và Truyền thông ban hành Quy chế về quản lý và sử dụng tài nguyên Internet;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ 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 964/QĐ-TTg ngày 10/8/2022 của Thủ tướng Chính phủ phê duyệt Chiến lược An toàn, An ninh quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn đến năm 2045;

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 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 3710/QĐ-BGDĐT ngày 16/11/2022 của Bộ Giáo dục và Đào tạo ban hành Quy chế đảm bảo an toàn thông tin mạng;

Căn cứ Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ ban hành Quy định chi tiết một số điều của Luật An ninh mạng;

Căn cứ Quyết định số 2397/QĐ-BTC ngày 06/11/2023 của Bộ Tài chính về ban hành Kế hoạch triển khai Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn đến năm 2030;

Căn cứ Nghị quyết số 13/NQ-ĐHTCM-HĐT ngày 28/9/2021 của Hội đồng trường Trường Đại học Tài chính – Marketing ban hành Quy chế tổ chức và hoạt động của Trường Đại học Tài chính – Marketing;

Theo đề nghị của Trưởng phòng Công nghệ thông tin.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này "Quy chế đảm bảo an toàn thông tin mạng của Trường Đại học Tài chính - Marketing".

Điều 2. Quyết định có hiệu lực thi hành kể từ ngày ký. Trưởng phòng Công nghệ thông tin, Trưởng các đơn vị và toàn thể viên chức, người lao động thuộc Trường chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 2;
- Lưu: VT, CNTT.

HIỆU TRƯỞNG

TRƯỜNG ĐẠI HỌC TÀI CHÍNH MARKETING

PGS.TS. Phạm Tiến Đạt

BỘ TÀI CHÍNH
TRƯỜNG ĐẠI HỌC
TÀI CHÍNH - MARKETING

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

QUY CHẾ

Đảm bảo an toàn thông tin mạng của Trường Đại học Tài chính - Marketing

(Ban hành kèm theo Quyết định số: 3250/QĐ-ĐHTCM ngày 06 tháng 12 năm 2023 của Hiệu trưởng Trường Đại học Tài chính - Marketing)

Chương I
QUY CHẾ CHUNG

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

1. Quy chế này quy định về đảm bảo an toàn thông tin mạng, chủ động ứng phó với các thách thức từ không gian mạng trong các hoạt động ứng dụng công nghệ thông tin và chuyển đổi số của Trường Đại học Tài chính – Marketing (sau đây gọi tắt là Trường).

2. Quy chế này áp dụng đối với:

a) Các tổ chức và đơn vị thuộc Trường.

b) Viên chức và người lao động thuộc Trường; sinh viên, học viên, nghiên cứu sinh đang học tập thuộc các bậc, chương trình đào tạo thuộc Trường (sau đây gọi tắt là cá nhân).

c) Cơ quan, tổ chức, cá nhân có cung cấp các dịch vụ Internet, dịch vụ đám mây, phần mềm ứng dụng có sử dụng hoặc kết nối truy cập vào hệ thống mạng của Trường.

Điều 2. Giải thích từ ngữ

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

1. Hệ thống mạng: bao gồm các dịch vụ và các nền tảng kết nối Internet; mạng nội bộ; mạng truyền dẫn số liệu chuyên dùng.

2. Mạng nội bộ (LAN): là tập hợp các thiết bị công nghệ thông tin được kết nối với nhau có dây hoặc không dây (wifi) thông qua các bộ chuyển mạch, bộ định tuyến, thiết bị truy cập, máy chủ, thiết bị quản lý mạng, phần mềm quản lý mạng, thiết bị bảo mật và an toàn thông tin trong hệ thống mạng thuộc phạm vi quản lý của Trường.

3. Phòng máy chủ: bao gồm hệ thống máy chủ, thiết bị chuyển mạch, thiết bị định tuyến, thiết bị lưu trữ, thiết bị bảo mật và an toàn thông tin mạng, thiết bị ngoại vi, thiết

bị phụ trợ, đường truyền kết nối Internet, thiết bị phòng cháy chữa cháy, chống sét, và các thiết bị khác hỗ trợ khác phục vụ vận hành và quản trị tại phòng máy chủ.

4. Mạng truyền dẫn số liệu chuyên dùng: là mạng của các cơ quan Đảng, Nhà nước, Bộ, ngành được sử dụng riêng trong hoạt động truyền dẫn số liệu, ứng dụng công nghệ thông tin và chuyển đổi số của các cơ quan Đảng, Nhà nước và các Bộ, ngành liên quan.

5. Trang thiết bị công nghệ thông tin cá nhân: bao gồm máy tính để bàn, máy tính xách tay (laptop), thiết bị số (máy tính bảng, điện thoại thông minh,...) của cá nhân hoặc thiết bị công nghệ thông tin do Trường cấp theo quy định.

6. Đơn vị vận hành hệ thống thông tin: là đơn vị chủ trì việc quản lý và vận hành kỹ thuật hệ thống thông tin theo chức năng, nhiệm vụ do Trường ban hành.

Điều 3. Phạm vi đảm bảo an toàn thông tin

1. Hệ thống máy chủ.

2. Hệ thống mạng.

3. Hệ thống thông tin quản lý bao gồm phần mềm phục vụ hoạt động quản trị Trường; các phần mềm nghiệp vụ và cơ sở dữ liệu; các nền tảng số phục vụ công tác quản lý, điều hành hoạt động chung toàn Trường; bảo đảm an toàn, an ninh mạng cho quá trình chuyển đổi số của Trường.

4. Dữ liệu của tổ chức, đơn vị và cá nhân thuộc Trường.

5. Trang thiết bị công nghệ thông tin cá nhân.

Điều 4. Nguyên tắc đảm bảo an toàn thông tin trên không gian mạng

1. Đảm bảo an toàn thông tin trên không gian mạng là yêu cầu bắt buộc, thường xuyên, liên tục đối với tổ chức, đơn vị và cá nhân thuộc Trường. Hệ thống thông tin phải được xây dựng đồng bộ, liên thông dữ liệu từ khâu thiết kế, xây dựng, vận hành, nâng cấp, hủy bỏ (dừng hoạt động).

2. Tuân thủ các nguyên tắc chung được quy định tại Điều 4 Luật An toàn thông tin mạng và Điều 4 Nghị định số 86/2016/NĐ-CP ngày 01/7/2016 của Chính phủ.

3. Đơn vị được Trường giao vận hành hệ thống thông tin và các đơn vị có liên quan có trách nghiệm đảm bảo an toàn thông tin mạng đối với hệ thống thông tin của đơn vị mình quản lý và sử dụng; bố trí nhân sự và phối hợp với các đơn vị thuộc Trường sẵn

sàng xử lý sự cố an toàn thông tin mạng đối với các hệ thống thông tin do đơn vị mình quản lý.

4. Các tổ chức, đơn vị và cá nhân thuộc Trường có trách nhiệm đảm bảo an toàn thông tin mạng trong phạm vi xử lý công việc của mình theo quy định của Trường và của Nhà nước.

5. Xử lý sự cố an toàn thông tin mạng phải phù hợp với trách nhiệm, quyền hạn và đảm bảo lợi ích hợp pháp của tổ chức, đơn vị, cá nhân thuộc Trường và theo quy định của pháp luật.

Điều 5. Các hành vi bị nghiêm cấm

1. Ngăn chặn việc truyền tải thông tin trên các nền tảng số của Trường; truy cập, gây nguy hại, xóa, thay đổi, sao chép, cắt ghép và làm sai lệch thông tin trên mạng trái pháp luật.

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

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

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

5. 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 của tổ chức, đơn vị và cá nhân.

6. Xâm nhập trái pháp luật, đánh cắp và sử dụng trái phép mật khẩu, khoá mật mã đã được mã hóa hợp pháp của tổ chức, đơn vị và cá nhân thuộc Trường.

7. Các hành vi bị nghiêm cấm quy định lại Điều 8 Luật An ninh mạng.

Chương II
QUY ĐỊNH ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 6. Đảm bảo an toàn thông tin tại phòng máy chủ và hệ thống mạng

1. Phòng Công nghệ thông tin là đơn vị quản lý, vận hành hệ thống máy chủ, hạ tầng mạng và dịch vụ Internet của Trường.

2. Phòng Công nghệ thông tin thường xuyên kiểm tra và giám sát kết nối mạng Internet của các thiết bị đầu cuối, phát hiện và ngăn chặn các hành vi xâm nhập tiềm ẩn rủi ro hoặc bất hợp pháp từ mạng Internet.

3. Phòng Công nghệ thông tin chủ động, phối hợp với các đơn vị có liên quan chủ động đề xuất các phương án đảm bảo an toàn cho hệ thống máy chủ, hệ thống mạng và các hệ thống thông tin thuộc Trường.

4. Phòng máy chủ là khu vực hạn chế tiếp cận; chỉ những cá nhân có quyền, nhiệm vụ theo phân công mới được phép vào phòng máy chủ.

Điều 7. Đảm bảo an toàn thông tin đối với các hệ thống thông tin và cơ sở dữ liệu của Trường

1. Các tổ chức, đơn vị và cá nhân thuộc Trường có trách nhiệm quản lý, bảo quản các thiết bị công nghệ thông tin và tài nguyên mạng lắp đặt tại phòng làm việc của đơn vị mình.

2. Khi phát hiện nguy cơ mất an toàn thông tin (cảnh báo từ phần mềm chống mã độc, máy tính hoạt động chậm bất thường, mất dữ liệu, mất quyền truy cập hệ thống,...), đơn vị và các nhân thuộc Trường phải tắt thiết bị công nghệ thông tin, kịp thời thông báo với Phòng Công nghệ thông tin để được hỗ trợ xử lý.

3. Khi xây dựng mới hoặc nâng cấp hệ thống thông tin, đơn vị quản lý hệ thống thông tin và các đơn vị liên quan có trách nhiệm sao lưu dữ liệu, rà soát cấp độ an toàn của hệ thống thông tin và thực hiện điều chỉnh, bổ sung cấp độ an toàn thông tin trong trường hợp cần thiết.

4. Đảm bảo an toàn thông tin khi đưa vào khai thác sử dụng hệ thống thông tin và cơ sở dữ liệu được thông suốt và an toàn.

Điều 8: Đảm bảo an toàn thông tin trong quản lý và sử dụng tài khoản truy cập các hệ thống thông tin của Trường

1. Khi được cấp tài khoản sử dụng các hệ thống thông tin của Trường, tổ chức, đơn vị và cá nhân phải đổi mật khẩu trong lần đăng nhập đầu tiên. Đặt mật khẩu có độ dài ít nhất 10 ký tự, gồm: chữ cái hoa và thường, ký tự số và ký tự đặc biệt; thay đổi mật khẩu theo định kỳ tối thiểu 01 lần/3 tháng. Tổ chức, đơn vị và cá nhân có trách nhiệm bảo mật thông tin tài khoản truy cập, không chia sẻ mật khẩu với người khác. Đăng xuất hệ thống

thông tin khi không sử dụng.

2. Đối cá nhân là viên chức, người lao động khi thay đổi vị trí công tác, chuyển công tác, thôi việc, nghỉ hưu, hoặc tạm khóa quyền truy cập tài khoản người dùng, Phòng Tổ chức – Hành chính thông báo cho đơn vị vận hành hệ thống thông tin thực hiện điều chỉnh, tạm khóa, thu hồi hoặc hủy bỏ tài khoản.

3. Đối với cá nhân là sinh viên, học viên, nghiên cứu sinh sau khi kết thúc khóa học, thôi học hoặc đã tốt nghiệp, các đơn vị có liên quan quản lý cá nhân đó phải thông báo cho đơn vị vận hành hệ thống thông tin thực hiện điều chỉnh, tạm khóa, thu hồi hoặc hủy bỏ tài khoản.

4. Phòng Công nghệ thông tin có quyền khóa, thu hồi 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 thông tin. Tài khoản của tổ chức, đơn vị đã giải thể hoặc tài khoản của cá nhân không còn làm việc hoặc học tập tại Trường sẽ được thu hồi sau 02 (hai) tuần khi nhận được thông báo từ Phòng Tổ chức - Hành chính.

Điều 9. Đảm bảo an toàn thông tin trang thiết bị công nghệ thông tin cá nhân

1. Cá nhân chịu trách nhiệm về đảm bảo an toàn thông tin liên quan đến tài khoản và thiết bị do mình được giao quản lý và sử dụng.

2. Các thiết bị công nghệ thông tin cá nhân phải được cài đặt và cập nhật thường xuyên phần mềm phòng chống mã độc; thực hiện kiểm tra, rà quét bằng phần mềm phòng chống mã độc khi sao chép, mở các tập tin trước khi kết nối các thiết bị lưu trữ dữ liệu di động với máy tính của mình.

3. Cá nhân chịu trách nhiệm và có biện pháp đảm bảo an toàn thông tin, tránh bị lộ lọt dữ liệu khi thực hiện bảo hành, bảo dưỡng, sửa chữa hoặc bảo trì thiết bị do mình quản lý.

4. Khi ngừng sử dụng thiết bị công nghệ thông tin cá nhân, cá nhân phải thực hiện sao lưu và tiêu hủy dữ liệu. Đối với dữ liệu của đơn vị và của Trường; thiết bị công nghệ thông tin do Trường cấp thì cá nhân thực hiện bàn giao theo quy định.

Điều 10. Ứng cứu sự cố an toàn hệ thống thông tin

1. Phòng Công nghệ thông tin chủ động và phối hợp với các đơn vị liên quan kiểm tra, đánh giá mức độ mất an toàn thông tin đối với hệ thống máy chủ, hệ thống mạng, các

hệ thống thông tin và cơ sở dữ liệu thuộc Trường và triển khai các phương án sao lưu dữ liệu nhanh nhất có thể.

2. Chủ động, báo cáo và đề xuất phương án ứng cứu sự cố an toàn thông tin theo quy định của Trường, của Bộ Tài chính và của Nhà nước.

3. Tham gia diễn tập ứng cứu sự cố an toàn thông tin mạng theo quy định của Trường, của Bộ Tài chính và của Nhà nước.

Chương III
TỔ CHỨC THỰC HIỆN

Điều 11. Trách nhiệm của các đơn vị thuộc Trường

1. Tổ chức phổ biến, chỉ đạo việc tuân thủ các quy định tại Quy chế này và các văn bản quy định có liên quan khác của Nhà nước đối với các cá nhân thuộc đơn vị mình về an toàn thông tin mạng.

2. Thường xuyên kiểm tra, đôn đốc việc triển khai an toàn thông tin mạng trong công việc của cá nhân do mình quản lý.

3. Thực hiện các báo cáo theo yêu cầu gửi Phòng Công nghệ thông tin, để tổng hợp, báo cáo Lãnh đạo Trường (nếu có).

Điều 12. Trách nhiệm của cá nhân

1. Thực hiện đầy đủ các quy định liên quan tại Quy chế này về đảm bảo an toàn thông tin mạng.

2. Tham gia các lớp bồi dưỡng kiến thức, kỹ năng về an toàn, an ninh mạng, tuyên truyền, phổ biến nâng cao nhận thức, diễn tập an toàn thông tin và ứng cứu sự cố để bảo đảm an toàn thông tin mạng theo kế hoạch của Trường hoặc của Bộ, ngành liên quan.

3. Chịu trách nhiệm trước pháp luật và Trường về các vi phạm làm mất an toàn thông tin mạng do không tuân thủ Quy chế này.

Điều 13. Trách nhiệm của Phòng Công nghệ thông tin

1. Lập kế hoạch hằng năm về triển khai công tác an toàn, an ninh mạng, chủ động ứng phó với các thách thức từ không gian mạng.

2. Đề xuất và lập kế hoạch đào tạo, phát triển nguồn nhân lực an toàn, an ninh mạng theo cấp độ.

3. Tham gia ý kiến với các Bộ, ngành về các văn bản quy định, hướng dẫn về an toàn, an ninh mạng.

4. Tổ chức theo dõi, đôn đốc, kiểm tra, giám sát và đánh giá việc thực hiện Quy chế này đối với tổ chức, đơn vị và cá nhân thuộc Trường.

5. Tổ chức triển khai các quy định bảo đảm an toàn thông tin mạng của Trường theo phân công tại Quy chế này.

6. Hỗ trợ các tổ chức, đơn vị và cá nhân về công tác bảo đảm an toàn, an ninh mạng.

7. Chủ động, báo cáo kịp thời các nguy cơ tiềm ẩm gây mất an toàn, an ninh mạng và phối hợp thực hiện với các cơ quan cấp trên theo quy định của pháp luật hiện hành.

Chương IV
ĐIỀU KHOẢN THI HÀNH

Điều 14. Điều khoản thực hiện

1. Quy chế đảm bảo an toàn thông tin mạng của Trường Đại học Tài chính - Marketing có hiệu lực kể từ ngày ký ban hành. Các Quy chế không đề cập trong văn bản này thì áp dụng theo Quy chế hiện hành của Nhà nước và các Bộ, ngành liên quan.

2. Các tổ chức, đơn vị, viên chức, người lao động, người học thuộc Trường có trách nhiệm thực hiện nghiêm túc và đầy đủ các quy định của Quy chế này.

3. Trong quá trình triển khai thực hiện, nếu có những vấn đề khó khăn, vướng mắc, các tổ chức, đơn vị và cá nhân phản hồi về Phòng Công nghệ thông tin để tổng hợp, trình Lãnh đạo Trường xem xét, phê duyệt sửa đổi, bổ sung Quy chế này./.