BỘ TÀI CHÍNH
**TRƯỜNG ĐẠI HỌC**
**TÀI CHÍNH – MARKETING**
Số: 1731/QĐ-ĐHTCM-QLTSCNTT

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

*Thành phố Hồ Chí Minh, ngày 03 tháng 6 năm 2025*

# QUYẾT ĐỊNH

**Ban hành Quy định quản lý, vận hành, khai thác hạ tầng công nghệ thông tin và hệ thống thông tin của Trường Đại học Tài chính – Marketing**

*Căn cứ Luật Công nghệ thông tin số 67/2006/QH11 ngày 29/6/2006 của Quốc hội;*

*Căn cứ Luật An ninh mạng số 24/2018/QH14 ngày 12/6/2018 của Quốc hội;*

*Căn cứ Luật Giao dịch điện tử số 20/2023/QH15 ngày 22/6/2023 của Quốc hội;*

*Căn cứ Thông tư số 39/2017/TT-BTTTT ngày 15/12/2017 của Bộ Thông tin và Truyền thông ban hành Danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước;*

*Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông 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;*

*Căn cứ Quyết định số 4279/QĐ-BGDĐT ngày 14/12/2022 của Bộ trưởng Bộ Giáo dục và Đào tạo ban hành Quy chế quản lý, vận hành, khai thác sử dụng hệ thống cơ sở dữ liệu giáo dục và đào tạo tại Bộ Giáo dục và Đào tạo;*

*Căn cứ Quyết định số 1434/QĐ-ĐHTCM ngày 31/5/2022 của Hiệu trưởng Trường Đại học Tài chính – Marketing về việc ban hành Quy định về tổ chức hoạt động của Trang thông tin điện tử Trường Đại học Tài chính – Marketing;*

*Căn cứ Quyết định số 1792/QĐ-ĐHTCM ngày 18/7/2022 của Hiệu trưởng Trường Đại học Tài chính – Marketing về việc ban hành Quy chế quản lý phòng thực hành và Nội quy phòng thực hành của Trường Đại học Tài chính – Marketing;*

*Căn cứ Quyết định số 3250/QĐ-ĐHTCM ngày 06/12/2023 của Hiệu trưởng Trường Đại học Tài chính – Marketing về việc ban hành Quy chế đảm bảo an toàn thông tin mạng của Trường Đại học Tài chính – Marketing;*

*Căn cứ Quyết định số 3619/QĐ-ĐHTCM ngày 26/12/2024 của Hiệu trưởng Trường Đại học Tài chính – Marketing về chức năng, nhiệm vụ, quyền hạn của Phòng Quản lý tài sản và Công nghệ thông tin thuộc Trường;*

*Theo đề nghị của Trưởng phòng Quản lý tài sản và Công nghệ thông tin.*

**QUYẾT ĐỊNH:**

**Điều 1**. Ban hành kèm theo Quyết định "Quản lý, vận hành, khai thác hạ tầng công nghệ thông tin và hệ thống thông tin của Trường Đại học Tài chính – Marketing".

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

***Nơi nhận:***
- Ban Giám hiệu;
- Như Điều 2;
- Lưu: VT, QLTSCNTT.

**HIỆU TRƯỞNG**

TRƯỜNG ĐẠI HỌC TÀI CHÍNH - MARKETING

**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 ĐỊNH

**Về quản lý, vận hành, khai thác hạ tầng công nghệ thông tin và hệ thống thông tin của Trường Đại học Tài chính – Marketing**

*(Ban hành kèm theo Quyết định số 1731/QĐ-ĐHTCM ngày 03 tháng 6 năm 2025 của Hiệu trưởng Trường Đại học Tài chính – Marketing)*

## Chương I

## QUY ĐỊNH CHUNG

### Điều 1. Phạm vi và đối tượng áp dụng

1. Quy định này quy định đối với toàn bộ hoạt động quản lý, vận hành, khai thác bảo trì và phát triển hạ tầng công nghệ thông tin, hệ thống thông tin, phần mềm ứng dụng, cơ sở dữ liệu và các dịch vụ công nghệ thông tin khác thuộc Trường Đại học Tài chính – Marketing (sau đây gọi tắt là Trường).

2. Quy định này áp dụng đối với các tổ chức và đơn vị thuộc và trực thuộc Trường; viên chức và người lao động, sinh viên, học viên, nghiên cứu sinh đang học tập thuộc các bậc, chương trình đào tạo của Trường (sau đây gọi tắt là đơn vị và cá nhân); các cơ quan, tổ chức, cá nhân có hợp tác và cung cấp các dịch vụ Internet, dịch vụ đám mây, dịch vụ giám sát, dịch vụ an toàn thông tin, phần mềm ứng dụng, cổng thanh toán và các dịch vụ khác có sử dụng hoặc kết nối truy cập vào hạ tầng công nghệ thông tin và các hệ thống thông tin của Trường (sau đây gọi tắt là nhà cung cấp dịch vụ bên ngoài).

### Điều 2. Giải thích từ ngữ

Trong phạm vi Quy định này, các từ ngữ dưới đây được hiểu như sau:

1. *Mạng nội bộ (LAN - Local Area Network)*: Là một loại mạng máy tính kết nối các thiết bị công nghệ thông tin trong một phạm vi nhỏ như: trong một phòng, một tòa nhà, một văn phòng hoặc khuôn viên trường học.

2. *Mạng diện rộng (WAN - Wide Area Network)*: Là một loại mạng máy tính kết nối các thiết bị công nghệ thông tin hoặc mạng diện rộng ở các vị trí địa lý khác nhau, có thể trải rộng trên thành phố, quốc gia hoặc toàn cầu.

3. *Mạng truyền dẫn số liệu chuyên dùng (Specialized Data Transmission Network)*: là hệ thống mạng được xây dựng và vận hành riêng biệt cho một tổ chức hoặc nhóm tổ chức cụ thể, nhằm truyền tải dữ liệu phục vụ công tác quản lý, điều hành, trao đổi thông tin nội bộ một cách an toàn và ổn định, không phụ thuộc vào mạng công cộng.

4. *Mạng riêng ảo (VPN - Virtual Private Network)*: Là một công nghệ cho phép thiết lập kết nối an toàn từ xa tới hệ thống mạng nội bộ của Trường thông qua kênh truyền được mã hóa, giúp bảo vệ dữ liệu và kiểm soát truy cập.

5. *Hệ thống mạng (Network System)*: Là một tập hợp các thiết bị máy tính và thiết bị mạng được kết nối với nhau thông qua các phương tiện truyền dẫn (như dây cáp, sóng vô tuyến, cáp quang,…) nhằm mục đích chia sẻ tài nguyên (dữ liệu, máy in, kết nối Internet, phần mềm,…) giữa các máy tính, máy chủ và thiết bị ngoại vi. Hệ thống mạng bao gồm: mạng LAN, mạng WAN, mạng truyền dẫn số liệu chuyên dùng, kết nối Internet và các thiết bị công nghệ thông tin liên quan.

6. *Thiết bị cá nhân (Personal Device)*: Là các thiết bị công nghệ thông tin thuộc sở hữu cá nhân của viên chức, người lao động, người học hoặc đối tác, không do Trường cấp phát, nhưng có thể được sử dụng để kết nối trực tiếp hoặc từ xa vào hệ thống mạng, hạ tầng công nghệ thông tin và các hệ thống thông tin của Trường. Thiết bị cá nhân bao gồm nhưng không giới hạn ở máy tính xách tay (laptop), điện thoại di động, máy tính bảng, thiết bị lưu trữ di động (USB, ổ cứng ngoài), thiết bị in ấn, thiết bị ngoại vi và các thiết bị công nghệ khác có khả năng truy cập hoặc lưu trữ dữ liệu của Trường.

7. *Thiết bị công nghệ thông tin (Information Technology Equipment)*: Là các thiết bị điện tử được sử dụng để thu thập, xử lý, lưu trữ, truyền tải và hiển thị thông tin dưới dạng số, phục vụ cho việc vận hành và quản lý hệ thống công nghệ thông tin. Thiết bị này bao gồm các thiết bị được Trường trang bị và quản lý như máy tính xách tay, máy tính để bàn, máy chủ, thiết bị mạng, thiết bị lưu trữ, thiết bị ngoại vi, thiết bị trình chiếu (máy chiếu, màn hình tương tác,…) và không bao gồm thiết bị cá nhân (xem định nghĩa tại mục 6 - Điều 2).

8. *Thiết bị đầu cuối (Endpoint Device)*: Là các thiết bị mà người dùng sử dụng để tương tác trực tiếp với hệ thống mạng hoặc hệ thống thông tin.

9. *Hệ thống thông tin (IS - Information System)*: Là tập hợp các thành phần gồm phần cứng, phần mềm, cơ sở dữ liệu, quy trình và con người, có chức năng thu thập, xử lý, lưu

trữ và cung cấp thông tin phục vụ công tác quản lý, đào tạo và nghiên cứu, công tác chuyên môn, công tác điều hành và quản trị của Trường.

10. *Hạ tầng công nghệ thông tin (Information Technology Infrastructure)*: Là tập hợp các tài nguyên vật lý và ảo bao gồm thiết bị phần cứng, phần mềm, mạng, lưu trữ dữ liệu và các thành phần bảo mật, nhằm hỗ trợ cho việc xây dựng, vận hành và quản lý các hệ thống thông tin trên các nền tảng số của Trường.

11. *Phòng máy chủ (Server Room)*: 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 hỗ trợ khác phục vụ vận hành và quản trị tại phòng máy chủ.

12. *Người quản trị hệ thống (SA - System Administrator)*: Là cá nhân được phân công hoặc ủy quyền để thực hiện các chức năng cấu hình, duy trì, giám sát, kiểm soát truy cập và đảm bảo an toàn, ổn định cho hệ thống thông tin (IS), phần mềm ứng dụng, máy chủ và các nền tảng số của Trường.

13. *Người dùng (User)*: là viên chức và người lao động, người học hiện đang công tác và theo học tại Trường; các nhà cung cấp dịch vụ bên ngoài được cấp quyền truy cập và sử dụng hạ tầng công nghệ thông tin và các hệ thống thông tin của Trường. Người dùng gồm người quản trị hệ thống, người dùng trong trường và người dùng là các nhà cung cấp dịch vụ bên ngoài.

14. *Tài nguyên công nghệ thông tin (Information Technology Resources)*: Bao gồm phần cứng, phần mềm, dữ liệu, tài khoản truy cập, dịch vụ mạng và các tiện ích công nghệ khác thuộc sở hữu hoặc quản lý của Trường.

15. *An toàn thông tin (Information Security)*: Là tập hợp các chính sách, quy trình, công nghệ và biện pháp kỹ thuật nhằm bảo vệ thông tin và hệ thống thông tin khỏi các mối đe dọa trên không gian mạng.

16. *Tài khoản người dùng (User Account)*: Là một tập hợp thông tin định danh (tên đăng nhập, mật khẩu, thông tin cá nhân, quyền truy cập) được sử dụng để xác thực và cấp quyền truy cập cho một cá nhân, đơn vị hoặc tổ chức khi sử dụng máy tính, hệ thống mạng hoặc phần mềm hoặc các ứng dụng và dịch vụ trên môi trường mạng.

17. Đơn vị phụ trách công nghệ thông tin và chuyển đổi số: Là đơn vị thuộc Trường, được giao nhiệm vụ tham mưu, xây dựng kế hoạch, quản lý, vận hành, khai thác, bảo trì

và phát triển hạ tầng công nghệ thông tin, hệ thống thông tin; đảm bảo an ninh mạng và hỗ trợ kỹ thuật cho giảng viên, viên chức, người lao động, người học và các đơn vị có liên quan của Trường.

**Điều 3. Phạm vi quản lý, vận hành, khai thác hạ tầng công nghệ thông tin và các hệ thống thông tin**

1. Hệ thống máy chủ vật lý và máy chủ ảo.

2. Hệ thống mạng và truyền dẫn số liệu.

3. Hạ tầng dịch vụ đám mây (nếu có).

4. Hệ thống thông tin và phần mềm ứng dụng trên các nền tảng số của Trường.

5. Dữ liệu của các đơn vị và cá nhân trong Trường.

6. Thiết bị công nghệ thông tin do Trường cấp và thiết bị cá nhân.

7. Giải pháp và công cụ bảo mật thông tin.

**Điều 4. Nguyên tắc quản lý, vận hành, khai thác hạ tầng công nghệ thông tin và hệ thống thông tin**

1. Hạ tầng công nghệ thông tin, các hệ thống thông tin và phần mềm ứng dụng trên các nền tảng số phải luôn duy trì hoạt động ổn định, thông suốt và bảo mật. Yêu cầu an toàn thông tin là bắt buộc, được thực hiện thường xuyên và liên tục đối với các đơn vị và cá nhân trong Trường.

2. Đơn vị được Trường giao quản lý, vận hành, khai thác hạ tầng công nghệ thông tin, các hệ thống thông tin, phần mềm ứng dụng và các đơn vị và cá nhân có liên quan có trách nhiệm đảm bảo an toàn thông tin mạng đối với hệ thống thông tin và phần mềm ứng dụng 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.

3. Các đơn vị và cá nhân trong Trường có trách nhiệm quản lý, vận hành, khai thác hạ tầng công nghệ thông tin, thiết bị công nghệ thông tin, hệ thống thông tin và phần mềm ứng dụng của Trường đảm bảo hiệu quả, tiết kiệm, an toàn thông tin mạng trong phạm vi xử lý công việc của mình theo quy định của Trường và các quy định hiện hành của Nhà nước.

**Điều 5. Các hành vi bị nghiêm cấm**

1. Hành vi cản trở trái phép việc truyền tải thông tin trên các nền tảng số của Trường; truy cập trái phép vào dữ liệu, gây nguy hại, xóa, thay đổi, sao chép, đánh cắp, cắt ghép và làm sai lệch thông tin trên môi trường mạng trái pháp luật.

2. Gây ảnh hưởng, cản trở trái pháp luật tới hoạt động bình thường của hạ tầng công nghệ thông tin, các hệ thống thông tin và phần mềm ứng dụng và khả năng truy cập hệ thống thông tin của người dùng thuộc Trường.

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

4. Phát tán thư rác, phần mềm chứa mã độc, thiết lập các hệ thống thông tin giả mạo, lừa đảo nhằm đánh cắp thông tin hoặc gây nhầm lẫn.

5. Thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin của đơn vị và thông tin cá nhân của người khác; lợi dụng sơ hở, điểm yếu của hạ tầng công nghệ thông tin, hệ thống thông tin và phần mềm ứng dụng để thu thập, khai thác thông tin của các đơn vị và cá nhân trong Trường.

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 các đơn vị và cá nhân trong Trường.

7. Ngoài các hành vi nêu trên, các hành vi vi phạm quy định tại Điều 8 Luật An ninh mạng cũng bị nghiêm cấm.

## Chương II

## HẠ TẦNG CÔNG NGHỆ THÔNG TIN

**Điều 6. Hệ thống máy chủ và hệ thống mạng**

1. Thường xuyên được kiểm tra, cập nhật bản vá, nâng cấp về hệ điều hành, phần mềm bảo mật, phần mềm diệt virus cho hệ thống máy chủ (máy chủ vật lý, máy chủ ảo). Các thiết bị mạng chuyên dụng và thiết bị tường lửa cho hệ thống máy chủ cần được cấu hình đúng và cập nhật bản quyền theo định kỳ.

2. Phải có hệ thống kiểm soát ra/vào, điều hòa nhiệt độ, độ ẩm, thiết bị phòng cháy chữa cháy, chống sét và thiết bị lưu điện cho máy chủ. Thực hiện sao lưu dữ liệu và có chế độ phân quyền người dùng nhằm tránh nguy cơ rò rỉ, sửa đổi cấu hình do lỗi thao tác.

3. Thường xuyên kiểm tra và giám sát kết nối Internet của thiết bị đầu cuối, phát hiện và ngăn chặn các hành vi xâm nhập tiềm ẩn rủi ro hoặc bất hợp pháp từ Internet. Thực hiện bảo trì, nâng cấp hệ thống mạng theo định kỳ 01 tháng/lần để kịp thời phát hiện và thay thế, nâng cấp các thiết bị mạng hư hỏng, không còn phù hợp nhằm đảm bảo hoạt động chung của Trường được ổn định và thông suốt.

4. Phải có đường truyền chính và đường truyền dự phòng cho hệ thống máy chủ và hệ thống mạng tại các cơ sở đào tạo thuộc Trường để duy trì kết nối cho hệ thống máy chủ và truy cập Internet và Wi-Fi tại các cơ sở đào tạo của Trường khi đường truyền chính gặp sự cố.

**Điều 7. Hệ thống thông tin và cơ sở dữ liệu của Trường**

1. Các đơn vị được giao quản lý hệ thống thông tin hoặc cơ sở dữ liệu chịu trách nhiệm bảo đảm tính toàn vẹn, bảo mật và an toàn của hệ thống. Cá nhân sử dụng phải tuân thủ đúng mục đích, không chia sẻ hoặc sử dụng trái phép thông tin.

2. Khi xây dựng mới hoặc nâng cấp hệ thống thông tin hoặc phần mềm ứng dụng, các đơn vị liên quan có trách nhiệm sao lưu dữ liệu của đơn vị mình quản lý.

3. Các hệ thống thông tin phải lưu trữ nhật ký truy cập (log) với thời gian lưu trữ tối thiểu 03 (ba) tháng. Các nhật ký hệ thống phải được bảo mật, chỉ có người quản trị có quyền truy xuất và phải được kiểm tra định kỳ tối thiểu 06 tháng/lần.

4. Khi phát hiện nguy cơ gây 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,…), các đơn vị và cá nhân thuộc Trường phải tắt thiết bị công nghệ thông tin, kịp thời thông báo đến Phòng Quản lý tài sản và Công nghệ thông tin trong thời gian chậm nhất là 01 (một) giờ để được hỗ trợ và xử lý.

5. Phòng Quản lý tài sản và Công nghệ thông tin phối hợp với nhà cung cấp tập huấn, hướng dẫn sử dụng và khai thác hiệu quả đối với các hệ thống thông tin, phần mềm ứng dụng và thiết bị công nghệ thông tin chuyên dùng cho các đơn vị và cá nhân thuộc Trường.

**Điều 8. Quản lý, vận hành và khai thác thiết bị công nghệ thông tin**

1. Các thiết bị và tài nguyên công nghệ thông tin chỉ được sử dụng cho đào tạo, nghiên cứu, công tác chuyên môn, công tác điều hành và quản trị của Trường. Nghiêm cấm sử dụng vào mục đích cá nhân trái quy định.

2. Nghiêm cấm cài đặt và sử dụng phần mềm không có bản quyền, không rõ nguồn gốc hoặc chứa mã độc; tự ý thay đổi cấu hình hệ thống hoặc kết nối thiết bị trái phép. Các đơn vị và cá nhân có trách nhiệm kiểm tra tính hợp lệ của phần mềm trước khi sử dụng, và phải tự chịu trách nhiệm đối với mọi hành vi cấu hình, cài đặt hệ thống hoặc thiết bị.

3. Thiết bị công nghệ thông tin phải được quản lý tài sản theo đúng quy định hiện hành của Trường. Việc điều chuyển, thay thế, thanh lý cần thực hiện đúng quy trình.

4. Các đơn vị và cá nhân trong Trường có trách nhiệm quản lý, bảo quản, khai thác đúng mục đích, hiệu quả và tiết kiệm đối với thiết bị công nghệ thông tin được cấp.

5. Các máy tính cá nhân, máy tính để bàn được cấp 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.

6. Các đơn vị và 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.

7. Khi đơn vị ngừng hoạt động hoặc giải thể, cá nhân không còn học tập hoặc làm việc tại Trường thì các đơn vị và cá nhân đó phải bàn giao đầy đủ thiết bị và dữ liệu số của đơn vị/cá nhân theo quy định của Trường.

8. Phòng Quản lý tài sản và Công nghệ thông tin chịu trách nhiệm hướng dẫn sử dụng thiết bị công nghệ thông tin thông dụng bao gồm: máy in, máy quét (scanner), máy tính, thiết bị lưu trữ dữ liệu di động cho các đơn vị và cá nhân thuộc Trường.

9. Phòng Quản lý tài sản và Công nghệ thông tin phối hợp với nhà cung cấp dịch vụ bên ngoài thực hiện tập huấn, hướng dẫn sử dụng và khai thác hiệu quả đối với thiết bị công nghệ thông tin chuyên dùng cho các đơn vị và cá nhân thuộc Trường.

**Điều 9. Quản lý và sử dụng tài khoản truy cập các hệ thống thông tin của Trường**

1. Các đơn vị và cá nhân trong Trường có trách nhiệm bảo quản và bảo mật tài khoản

được cấp, không chia sẻ hoặc để lộ thông tin truy cập hệ thống.

2. Các đơn vị và cá nhân trong Trường khi được cấp tài khoản truy cập các hệ thống thông tin trên các nền tảng số của Trường phải đổi mật khẩu trong lần đăng nhập đầu tiên. Không sử dụng lại mật khẩu cũ và đặt mật khẩu có độ dài ít nhất 10 ký tự, gồm: chữ cái hoa, chữ cái thường, ký tự số và ký tự đặc biệt. Người dùng phải đổi mật khẩu ngay lần đăng nhập đầu tiên và định kỳ 03 tháng/lần, không chia sẻ mật khẩu và đảm bảo bảo mật tuyệt đối thông tin truy cập. Đăng xuất hệ thống thông tin khi không sử dụng.

3. 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, Phòng Tổ chức - Hành chính có trách nhiệm thông báo cho Phòng Quản lý tài sản và Công nghệ thông tin thực hiện điều chỉnh, tạm khóa, thu hồi hoặc hủy bỏ tài khoản theo quy định.

4. 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 có trách nhiệm thông báo cho Phòng Quản lý tài sản và Công nghệ thông tin thực hiện điều chỉnh, tạm khóa, thu hồi hoặc hủy bỏ tài khoản theo quy định.

5. Tài khoản quản trị hệ thống, tài khoản truy cập hệ thống, máy chủ phải được quản lý riêng biệt, lưu log đầy đủ và hạn chế quyền ở mức tối thiểu cần thiết.

6. Phòng Quản lý tài sản và Công nghệ thông tin có quyền khóa, thu hồi quyền truy cập tài khoản của các đơn vị và cá nhân thuộc Trường trong các trường hợp sau: tài khoản đó thực hiện các hành vi tấn công, nghi ngờ tài khoản bị chiếm quyền truy cập. Tài khoản được cấp của đơn vị đã giải thể, hợp nhất, sáp nhập hoặc tài khoản người dùng chấm dứt hoạt động tại Trường sẽ được thu hồi sau 14 ngày kể từ thời điểm kết thúc, trừ khi có yêu cầu khác từ đơn vị quản lý.

7. Phòng Quản lý tài sản và Công nghệ thông tin thực hiện rà soát và kiểm tra định kỳ tài khoản tối thiểu 06 tháng/lần hoặc đột xuất theo yêu cầu đối với tài khoản truy cập, thiết bị và phần mềm đảm bảo an toàn thông tin.

**Điều 10. Ứng cứu sự cố an toàn hạ tầng công nghệ thông tin và các hệ thống thông tin**

1. Phòng Quản lý tài sản và Công nghệ thông tin, Đội ứng cứu an toàn thông tin mạng 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, phần mềm ứng dụng,

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

2. Chủ động phối hợp với các đơn vị trong Trường và các nhà cung cấp dịch vụ bên ngoài tiến hành đánh giá, phân loại và xử lý sự cố theo cấp độ an toàn thông tin mạng.

3. Thực hiện quy trình ứng phó sự cố an toàn thông tin mạng tại phụ lục đính kèm theo Kế hoạch số 1385/KH-ĐHTCM-QLTSCNTT ngày 08/5/2025 của Ban Giám hiệu Trường Đại học Tài chính – Marketing về việc ứng phó sự cố, bảo đảm an toàn thông tin mạng tại Trường Đại học Tài chính – Marketing.

4. 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 các cơ quan cấp trên theo quy định hiện hành của nhà nước.

**Điều 11. Quản lý, vận hành, khai thác, bảo trì, nâng cấp hạ tầng công nghệ thông tin và hệ thống thông tin**

1. Phòng Quản lý tài sản và Công nghệ thông tin có trách nhiệm lập kế hoạch, kiểm tra, bảo trì hệ thống mạng, máy chủ, thiết bị công nghệ thông tin và hệ thống thông tin theo định kỳ.

2. Đầu tư, nâng cấp, thay thế hoặc tích hợp hệ thống thông tin, thiết bị công nghệ thông tin phải phù hợp với chiến lược phát triển của Trường, được thẩm định và phê duyệt theo đúng quy trình.

3. Mọi thay đổi về kỹ thuật (thay đổi cấu hình mạng, máy chủ, phần mềm hệ thống...) đều phải được ghi nhận, đánh giá rủi ro và ý kiến của Phòng Quản lý tài sản và Công nghệ thông tin.

4. Khi có sự cố, đơn vị sử dụng có trách nhiệm thông báo kịp thời để đơn vị phụ trách công nghệ thông tin xử lý. Các sự cố nghiêm trọng phải được báo cáo kịp thời cho Ban Giám hiệu.

**Điều 12. Bảo mật và an toàn thông tin**

1. 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.

2. Hệ thống máy chủ, thiết bị mạng đặt tại các phòng server của các cơ sở phải đảm bảo điều kiện về điện, nhiệt độ, độ ẩm và kiểm soát truy cập.

3. Phòng máy chủ phải có hệ thống camera giám sát 24/7 và dữ liệu camera phải được lưu trữ tối thiểu 14 ngày liên tục. Việc truy xuất dữ liệu camera chỉ được thực hiện bởi người có thẩm quyền hoặc theo yêu cầu của Lãnh đạo Trường hoặc đơn vị điều tra sự cố.

4. Áp dụng các giải pháp kỹ thuật để ngăn ngừa truy cập trái phép, mã độc, tấn công mạng; sử dụng phần mềm diệt virus và hệ thống giám sát an toàn.

5. Cơ sở dữ liệu trên máy chủ và dịch vụ đám mây phải được sao lưu định kỳ, đảm bảo khả năng phục hồi trong trường hợp xảy ra sự cố kỹ thuật, thiên tai hoặc hỏa hoạn.

6. Các đơn vị và cá nhân thuộc Trường thực hiện sao lưu định kỳ dữ liệu của đơn vị và cá nhân.

7. Việc cấp quyền truy cập hệ thống, dữ liệu phải căn cứ vào chức năng, nhiệm vụ của người sử dụng. Hoạt động này do Phòng Quản lý tài sản và Công nghệ thông tin kiểm soát. Mọi hành vi truy cập sai mục đích, rò rỉ và mất mát dữ liệu đều bị xử lý.

8. Người dùng sử dụng thiết bị cá nhân truy cập vào mạng, hệ thống thông tin và cơ sở dữ liệu của Trường phải tuân thủ các quy định về bảo mật, an toàn thông tin và chính sách kiểm soát truy cập do Trường ban hành. Thiết bị cá nhân phải được cài đặt phần mềm bảo mật hợp lệ trước khi truy cập vào các hệ thống của Trường. Người dùng phải đăng xuất khỏi hệ thống sau khi hoàn thành công việc.

9. Nhà cung cấp dịch vụ bên ngoài phải cam kết bảo mật thông tin theo các hợp đồng, biên bản ghi nhớ hợp tác đã ký kết hoặc theo yêu cầu của Trường, có trách nhiệm phối hợp khắc phục khi xảy ra sự cố an toàn thông tin.

10. Mọi truy cập từ xa (remote access) vào mạng LAN của Trường phải thông qua VPN hoặc các ứng dụng cho phép truy cập từ xa do Phòng Quản lý tài sản và Công nghệ thông tin quản lý. Thiết bị sử dụng VPN phải đáp ứng các tiêu chuẩn bảo mật về phần mềm, tường lửa cá nhân, cấu hình hệ thống và bản vá an ninh cập nhật.

**Điều 13. Kiểm tra đánh giá an toàn thông tin mạng và chế độ báo cáo**

1. Việc kiểm tra đánh giá an toàn thông tin mạng thực hiện theo Quy chế đảm bảo an toàn thông tin mạng và Quy trình ứng cứu sự cố an toàn thông tin mạng của Trường Đại học Tài chính – Marketing. Đối với các hệ thống thông tin quan trọng, Trường cần tổ chức diễn tập ứng phó an toàn thông tin mạng định kỳ tối thiểu 01 lần/năm nhằm phát hiện, khắc phục các lỗ hổng an ninh. Việc diễn tập có thể phối hợp với các đơn vị chuyên trách ngoài

Trường để đánh giá khách quan hiệu quả ứng phó và năng lực kỹ thuật nội bộ.

2. Các thiết bị lưu trữ di động khi lưu dữ liệu quan trọng, nhạy cảm (nhân sự, tài chính,...) phải được mã hóa. Trường hợp mất thiết bị, đơn vị và cá nhân phải thông báo đến Phòng Quản lý tài sản và Công nghệ thông tin trong vòng 01 giờ.

3. Thực hiện chế độ báo cáo định kỳ về tình trạng hệ thống và an toàn thông tin 06 tháng/lần hoặc đột xuất theo yêu cầu từ Lãnh đạo Trường hoặc cơ quan cấp trên.

## Chương III

## TỔ CHỨC THỰC HIỆN

**Điều 14. Trách nhiệm của các đơn vị thuộc Trường**

1. Tổ chức phổ biến, chỉ đạo việc tuân thủ các quy định này và các văn bản quy định có liên quan khác của Nhà nước đối với các cá nhân thuộc đơn vị mình phụ trách về quản lý, vận hành, khai thác hạ tầng công nghệ thông tin và các hệ thống thông tin của Trường.

2. Thường xuyên kiểm tra, đôn đốc việc quản lý, vận hành, khai thác hạ tầng công nghệ thông tin, thiết bị công nghệ thông tin, các hệ thống thông tin và phần mềm ứng dụng trên các nền tảng số của cá nhân do mình quản lý.

3. Có trách nhiệm phối hợp với Phòng Quản lý tài sản và Công nghệ thông tin trong việc triển khai các hệ thống, cung cấp dữ liệu, nội dung và kiểm soát thông tin thuộc lĩnh vực chuyên môn.

4. Tuân thủ các hướng dẫn kỹ thuật, quy trình quản lý, vận hành, khai thác hạ tầng công nghệ thông tin, các hệ thống thông tin, phần mềm ứng dụng, sử dụng tài khoản truy cập và đảm bảo an toàn thông tin trên không gian mạng.

5. Thực hiện các báo cáo theo đề nghị gửi Phòng Quản lý tài sản và Công nghệ thông tin, để tổng hợp, báo cáo Lãnh đạo Trường (nếu có).`

**Điều 15. Trách nhiệm của cá nhân thuộc Trường**

1. Có trách nhiệm sử dụng hệ thống đúng mục đích, đúng quyền hạn được phân công và tuân thủ đầy đủ các quy định về an toàn, bảo mật thông tin.

2. Không được tự ý cài đặt, thay đổi, sao chép, chia sẻ phần mềm hoặc truy cập vào các vùng dữ liệu trái phép.

3. Kịp thời thông báo cho đơn vị phụ trách công nghệ thông tin khi phát hiện sự cố kỹ thuật, hành vi nghi ngờ gây mất an toàn thông tin hoặc nguy cơ rủi ro hệ thống.

4. Chịu trách nhiệm trước pháp luật và Nhà trường về các vi phạm làm gián đoạn hệ thống mạng, máy chủ, hệ thống thông tin, phần mềm ứng dụng và gây mất an toàn thông tin mạng do không tuân thủ Quy định này.

**Điều 16. Trách nhiệm của Phòng Quản lý tài sản và Công nghệ thông tin**

1. Là đơn vị phụ trách công nghệ thông tin và chuyển đổi số của Trường và là đầu mối tham mưu, tổ chức và triển khai các hoạt động ứng dụng công nghệ thông tin và chuyển đổi số của Trường.

2. Quản lý, vận hành và phát triển hệ thống CNTT toàn Trường, bao gồm: máy chủ, mạng, thiết bị, phần mềm và dữ liệu. Đảm bảo hạ tầng công nghệ thông tin và hệ thống thông tin hoạt động ổn định, thông suốt và an toàn.

3. Tập huấn, hướng dẫn và hỗ trợ kỹ thuật:

a) Định kỳ tổ chức hoặc phối hợp với nhà cung cấp dịch vụ bên ngoài thực hiện tập huấn, hướng dẫn sử dụng phần mềm, thiết bị, hệ thống công nghệ thông tin cho các đơn vị và cá nhân thuộc Trường.

b) Hỗ trợ kỹ thuật cho các thiết bị công nghệ thông tin thông dụng và chuyên dùng.

4. Người quản trị hệ thống là viên chức thuộc Phòng Quản lý tài sản và Công nghệ thông tin được phân công và thực hiện việc cấu hình, giám sát, kiểm soát truy cập hệ thống thông tin. Người quản trị SA sẽ thực hiện phân quyền người dùng theo chức năng, nhiệm vụ của các đơn vị và cá nhân thuộc Trường liên quan đến quản lý và khai thác các hệ thống thông tin, phần mềm ứng dụng trên các nền tảng số của Trường.

5. Phối hợp triển khai, xử lý sự cố và đảm bảo an toàn thông tin:

a) Chủ trì phối hợp với các đơn vị liên quan trong xử lý sự cố mạng, bảo mật và triển khai các hoạt động ứng dụng công nghệ thông tin.

b) Phối hợp với nhà cung cấp dịch vụ bên ngoài để đánh giá, ứng cứu và phục hồi dữ liệu khi cần thiết.

6. Xây dựng và đề xuất kế hoạch phát triển, đầu tư, nâng cấp hạ tầng CNTT phù hợp với chiến lược phát triển của Trường và quy định pháp luật.

7. Kiểm tra, giám sát và đánh giá định kỳ:

a) Thực hiện kiểm tra tài khoản, nhật ký truy cập, cấu hình thiết bị, mạng và hệ thống bảo mật.

b) Giám sát tình trạng vận hành và an toàn thông tin theo kế hoạch định kỳ hoặc yêu cầu đột xuất.

8. Xây dựng kế hoạch đào tạo định kỳ tối thiểu 01 lần/năm cho cá nhân và nhân sự

chuyên trách công nghệ thông tin của Trường. Nội dung đào tạo bao gồm: bảo mật cá nhân, nhận diện mã độc, quản trị hệ thống và cập nhật thông tin lên website đơn vị.

9. Tổ chức theo dõi, đôn đốc, kiểm tra, giám sát và đánh giá việc thực hiện Quy chế này đối với các đối tượng liên quan trong Trường.

10. Chủ động, báo cáo kịp thời các nguy cơ tiềm ẩn gây mất an toàn đối với hạ tầng công nghệ thông tin, mạng và phối hợp thực hiện với các cơ quan cấp trên theo quy định của pháp luật hiện hành.

11. Tham gia ý kiến về các văn bản quy định, hướng dẫn về quản lý, vận hành, khai thác hạ tầng công nghệ thông tin và hệ thống thông tin của các Bộ, ngành.

**Điều 17. Trách nhiệm của nhà cung cấp dịch vụ bên ngoài**

1. Phối hợp với các đơn vị trong Trường ứng cứu khi có sự cố gây mất an toàn hạ tầng công nghệ thông tin và các hệ thống thông tin của Trường.

2. Nhà cung cấp phải thực hiện các biện pháp khắc phục, sao lưu, khôi phục dữ liệu và đảm bảo hệ thống vận hành an toàn theo đúng thời hạn được quy định trong các hợp đồng đã ký kết với Trường.

3. Nhà cung cấp phải chịu trách nhiệm về mọi hành vi vi phạm phát sinh từ tài khoản hoặc hệ thống do nhà cung cấp quản lý và có trách nhiệm hỗ trợ truy xuất, truy vết khi xảy ra sự cố an toàn thông tin.

4. Trường hợp phát hiện nhà cung cấp dịch vụ bên ngoài vi phạm nghĩa vụ bảo mật thông tin hoặc có hành vi tiềm ẩn nguy cơ gây mất an toàn hệ thống, Trường có quyền tạm thời đình chỉ quyền truy cập, ngắt kết nối dịch vụ để ngăn chặn rủi ro và bảo vệ hạ tầng công nghệ thông tin và hệ thống thông tin. Sau khi tiến hành đánh giá mức độ vi phạm, Trường sẽ ban hành văn bản yêu cầu nhà cung cấp dịch vụ giải trình, thực hiện khắc phục và triển khai các biện pháp xử lý phù hợp theo quy định tại hợp đồng đã ký kết và các quy định của pháp luật hiện hành.

**Điều 18. Xử lý vi phạm và khen thưởng**

1. Khen thưởng kịp thời các đơn vị và cá nhân phát hiện và báo cáo kịp thời các lỗ hổng gây gián đoạn hoặc mất an toàn đối với hạ tầng công nghệ thông tin, hệ thống thông tin và phần mềm ứng dụng trên các nền tảng số của Trường.

2. Các đối tượng liên quan trong Trường vi phạm quy định về quản lý, vận hành, khai thác hạ tầng công nghệ thông tin và các hệ thống thông tin, tùy theo mức độ vi phạm, sẽ bị xử lý kỷ luật, xử phạt hành chính hoặc truy cứu trách nhiệm theo nội quy, quy chế hiện hành của Trường và quy định của pháp luật.

3. Đối với nhà cung cấp dịch vụ bên ngoài, tùy theo mức độ vi phạm, Trường sẽ thực hiện xử lý theo các nội dung quy định trong hợp đồng và có thể yêu cầu bồi thường thiệt hại theo quy định của pháp luật.

## Chương IV

## ĐIỀU KHOẢN THI HÀNH

**Điều 19. Hiệu lực thi hành**

1. Quy định Quản lý, vận hành, khai thác hạ tầng công nghệ thông tin và hệ thống thông tin của Trường Đại học Tài chính – Marketing có hiệu lực kể từ ngày ký ban hành. Các nội dung không được đề cập trong Quy định này thì áp dụng theo các quy định hiện hành của Nhà nước và các Bộ, ngành liên quan.

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

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