BỘ TÀI CHÍNH
TRƯỜNG ĐẠI HỌC
TÀI CHÍNH - MARKETING

Số: 3684/QĐ-ĐHTCM

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

Thành phố Hồ Chí Minh, ngày 10 tháng 11 năm 2025

QUYẾT ĐỊNH

Ban hành Quy chế An toàn thông tin và An ninh mạng của Trường Đại học Tài chính - Marketing

HIỆU TRƯỞNG TRƯỜNG ĐẠI HỌC TÀI CHÍNH - MARKETING

Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19/11/2015 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 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 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 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 của Chính phủ ngày 15 tháng 7 năm 2013 về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng;

Căn cứ Nghị định số 42/2022/NĐ-CP ngày 24/6/2022 của Chính phủ về cung cấp thông tin và dịch vụ công trực tuyến của cơ quan Nhà nước;

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

Căn cứ Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về bảo vệ dữ liệu cá nhân;

Căn cứ Quyết định số 451/QĐ-TTg ngày 27/4/2020 của Thủ tướng Chính phủ ban hành Kế hoạch ứng cứu sự cố an toàn thông tin mạng quốc gia giai đoạn

2020-2025;

Căn cứ Quyết định số 1191/QĐ-TTg ngày 03/7/2023 của Thủ tướng Chính phủ phê duyệt Chiến lược An toàn, An ninh mạng quốc gia đến năm 2030, tầm nhìn đến năm 2050;

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 Thông tư số 21/2021/TT-BTTTT ngày 08/12/2021 của Bộ Thông tin và Truyền thông về quản lý, sử dụng tài nguyên Internet;

Căn cứ Quyết định số 3710/QĐ-BGDĐT ngày 16/11/2022 của Bộ trưởng Bộ Giáo dục và Đào tạo ban hành Quy chế đảm bảo an toàn thông tin mạng trong các cơ sở giáo dục;

Căn cứ Quyết định số 2405/QĐ-BTC ngày 08/7/2025 của Bộ trưởng Bộ Tài chính ban hành Quy chế An toàn thông tin và An ninh mạng;

Căn cứ Quyết định số 2872/QĐ-BTC ngày 21/8/2025 của Bộ trưởng Bộ Tài chính ban hành Kế hoạch bảo đảm an toàn, an ninh mạng tổng thể giai đoạn 2025-2030;

Căn cứ Quyết định số 1207/QĐ-ĐHTCM ngày 16/4/2025 của Hiệu trưởng Trường Đại học Tài chính - Marketing về việc thành lập Đội ứng cứu sự cố an toàn thông tin mạng của Trường;

Căn cứ Quyết định số 1731/QĐ-ĐHTCM-QLTSCNTT ngày 03/6/2025 của Hiệu trưởng Trường Đại học Tài chính - Marketing ban hành Quy chế quản lý, vận hành, khai thác hạ tầng công nghệ thông tin và hệ thống thông tin của Trường;

Theo đề nghị của Viện trưởng Viện Đổi mới sáng tạo và Chuyển đổi số.

QUYẾT ĐỊNH:

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

Điều 2. Quyết định có hiệu lực thi hành kể từ ngày ký và thay thế Quyết định số 3250/QĐ-ĐHTCM ngày 06/12/2023 về việc ban hành Quy chế bảo đảm an toàn thông tin mạng của Trường. Trưởng các đơn vị thuộc Trường, toàn thể viên chức, người lao động và người học thuộc Trường Đại học Tài chính - Marketing chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Ban Giám hiệu;
- Như Điều 2;
- Website UFM;
- Lưu: VT, ĐMSTCĐS (02b).

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 CHẾ

An toàn thông tin và An ninh mạng của Trường Đại học Tài chính – Marketing

(Ban hành kèm theo Quyết định số 3684/QĐ-ĐHTCM ngày 10 tháng 11 năm 2025 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 An toàn thông tin và An ninh mạng trong toàn Trường Đại học Tài chính – Marketing (sau đây gọi tắt là Trường); là cơ sở để tổ chức triển khai, quản lý, vận hành, kiểm tra, giám sát, ứng cứu và xử lý sự cố đối với các hệ thống thông tin, mạng máy tính, thiết bị công nghệ thông tin, phần mềm, cơ sở dữ liệu, dịch vụ trực tuyến và các tài nguyên thông tin khác thuộc phạm vi quản lý của Trường.

2. Quy chế này áp dụng đối với:

a) Các tổ chức và đơn vị thuộc và trực thuộc Trường.

b) Viên chức, người lao động và người học (sinh viên, học viên, nghiên cứu sinh) đang học tập, làm việc tại Trường (sau đây gọi tắt là cá nhân).

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

Điều 2. Giải thích từ ngữ

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

1. *An toàn thông tin mạng (ATTTM)*: là việc bảo vệ thông tin, hệ thống thông tin tránh khỏi truy cập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép, nhằm bảo đảm tính bí mật, toàn vẹn và sẵn sàng của thông tin.

2. *An ninh mạng (ANM)*: là việc bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội; bao gồm bảo vệ hệ thống thông tin

quan trọng về an ninh quốc gia và ngăn chặn, xử lý các hành vi xâm phạm theo quy định của pháp luật.

3. *Hệ thống thông tin*: là tập hợp phần cứng, phần mềm, cơ sở dữ liệu, mạng viễn thông và con người nhằm thu thập, xử lý, lưu trữ, truyền tải và trao đổi thông tin. Hệ thống thông tin bao gồm các hệ thống thông tin do Trường quản lý, vận hành tập trung và các hệ thống thông tin do đơn vị trực thuộc phát triển, quản lý, sử dụng theo chức năng, nhiệm vụ được giao. Việc định danh và phân loại hệ thống thông tin do Viện Đổi mới sáng tạo và Chuyển đổi số hướng dẫn thực hiện.

4. *Không gian mạng*: là môi trường được tạo lập bởi hạ tầng viễn thông, Internet, mạng máy tính, hệ thống thông tin, cơ sở dữ liệu, phần mềm và các thiết bị điện tử, trong đó con người tiến hành các hoạt động giao tiếp, học tập, làm việc và trao đổi thông tin không giới hạn bởi không gian và thời gian.

5. *Hệ thống mạng*: bao gồm hạ tầng kết nối, thiết bị mạng, các dịch vụ và nền tảng Internet, mạng nội bộ (LAN) và mạng truyền dẫn số liệu chuyên dùng.

6. *Mạng nội bộ (LAN)*: tập hợp các thiết bị công nghệ thông tin kết nối với nhau bằng dây hoặc không dây trong phạm vi giới hạn của Trường.

7. *Phòng máy chủ*: bao gồm máy chủ, thiết bị lưu trữ, bảo mật, thiết bị phụ trợ, đường truyền Internet và các thiết bị an toàn (thiết bị phòng cháy chữa cháy, thiết bị chống sét và kiểm soát ra vào).

8. *Mạng truyền dẫn số liệu chuyên dùng*: mạng của cơ quan Đảng, Nhà nước, Bộ, ngành trong hoạt động công nghệ thông tin, được kết nối, liên thông theo quy định.

9. *Trang thiết bị công nghệ thông tin cá nhân*: bao gồm máy tính để bàn, máy tính xách tay, máy tính bảng, điện thoại thông minh và thiết bị ngoại vi khác do cá nhân sở hữu hoặc được Trường cấp phát để phục vụ hoạt động giảng dạy, học tập, nghiên cứu, công tác chuyên môn và quản trị.

10. *Đơn vị vận hành hệ thống thông tin*: đơn vị được giao nhiệm vụ quản lý, vận hành kỹ thuật các hệ thống thông tin.

11. *Cấp độ an toàn hệ thống thông tin*: mức độ phân loại hệ thống thông tin theo quy định của pháp luật, gắn với yêu cầu bảo đảm an toàn tương ứng.

12. *Rủi ro an toàn, an ninh mạng*: khả năng xuất hiện sự cố gây mất an toàn thông tin mạng, an ninh mạng từ lỗ hổng, điểm yếu hoặc hành vi tấn công.

13. *Điểm yếu, lỗ hổng bảo mật*: thiếu sót trong thiết kế, triển khai hoặc vận hành hệ thống có thể bị lợi dụng, khai thác.

14. *Sự cố an toàn thông tin*: sự kiện hoặc hành vi ảnh hưởng tiêu cực đến tính bí mật, toàn vẹn, sẵn sàng của thông tin hoặc hệ thống thông tin.

15. *Mã độc (malware)*: là phần mềm hoặc đoạn mã được tạo ra với mục đích gây hại, phá hoại, đánh cắp hoặc chiếm quyền kiểm soát hệ thống, dữ liệu.

16. *Ứng cứu sự cố an toàn thông tin*: hoạt động phát hiện, phân tích, xử lý, khắc phục và phục hồi hệ thống sau sự cố.

17. *Trung tâm Giám sát, điều hành an toàn thông tin (SOC)*: bộ phận hoặc dịch vụ giám sát, cảnh báo, phân tích và ứng cứu sự cố tập trung; có thể do Trường tổ chức hoặc thuê ngoài.

18. *Dữ liệu cá nhân*: là thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự gắn liền với một cá nhân hoặc giúp nhận dạng cá nhân đó, theo quy định tại Nghị định số 13/2023/NĐ-CP.

19. *Tài khoản truy cập*: là thông tin định danh (tên đăng nhập, mật khẩu, mã xác thực hoặc phương thức khác) được cấp cho cá nhân hoặc đơn vị để sử dụng các hệ thống thông tin của Trường.

Điều 3. Phạm vi đảm bảo an toàn thông tin

1. Hệ thống máy chủ của Trường.

2. Hệ thống mạng, bao gồm mạng nội bộ (LAN), hạ tầng kết nối Internet và các mạng chuyên dùng được kết nối với Trường.

3. Các hệ thống thông tin và phần mềm ứng dụng phục vụ công tác đào tạo, nghiên cứu khoa học, quản lý, điều hành và các hoạt động chuyển đổi số của Trường.

4. Dữ liệu của tổ chức, đơn vị và cá nhân thuộc Trường, bao gồm cả dữ liệu cá nhân theo quy định pháp luật.

5. Trang thiết bị công nghệ thông tin cá nhân khi kết nối hoặc truy cập vào hệ thống mạng, dịch vụ thông tin của Trường.

6. Các hộp thư điện tử, tài khoản truy cập và dịch vụ trực tuyến được Trường cấp cho viên chức, người lao động, người học và các cá nhân có liên quan.

7. Các dịch vụ và nền tảng điện toán đám mây, phần mềm dịch vụ (SaaS) có lưu trữ,

xử lý hoặc kết nối với dữ liệu, hệ thống thông tin của Trường.

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 đến khi nâng cấp hoặc hủy bỏ hệ thống.

2. Tuân thủ các nguyên tắc chung của Luật An toàn thông tin mạng, Luật An ninh mạng, Nghị định số 53/2022/NĐ-CP và các văn bản pháp luật liên quan.

3. Mọi hoạt động thu thập, xử lý, lưu trữ và khai thác dữ liệu cá nhân phải tuân thủ Nghị định số 13/2023/NĐ-CP và các quy định pháp luật hiện hành.

4. Đơn vị được Trường giao vận hành hệ thống thông tin và các đơn vị có liên quan có trách nhiệm 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.

5. Các tổ chức, đơn vị và cá nhân thuộc Trường có trách nhiệm đảm bảo an toàn thông tin và an ninh mạng trong phạm vi xử lý công việc của mình theo quy định của Trường; đồng thời tuân thủ quy định của pháp luật hiện hành.

6. Thực hiện các biện pháp phòng ngừa, giám sát và ứng cứu nhằm hạn chế tối đa rủi ro, sự cố từ không gian mạng.

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

Điều 5. Các hành vi bị nghiêm cấm

1. Xâm nhập, phá hoại hệ thống

a) Truy cập trái phép vào hệ thống thông tin, gây nguy hại, xóa, thay đổi, sao chép hoặc làm sai lệch dữ liệu.

b) Tấn công, phát tán mã độc, virus hoặc các hình thức phá hoại khác.

2. Lạm dụng tài khoản và thông tin định danh

a) Sử dụng trái phép mật khẩu, khóa mật mã, chứng thư số hoặc thông tin định danh của tổ chức, cá nhân khác.

b) Che giấu hoặc không báo cáo sự cố mất an toàn thông tin khi phát hiện.

3. Sử dụng thiết bị, phần mềm trái phép

a) Không tự ý gắn, kết nối, cài đặt hoặc sử dụng thiết bị mạng, thiết bị công nghệ thông tin vào hệ thống khi chưa được đơn vị quản lý vận hành cho phép.

b) Sử dụng thiết bị lưu trữ hoặc phần mềm không rõ nguồn gốc, gây nguy cơ mất an toàn thông tin.

4. Phát tán hoặc chia sẻ thông tin sai trái, độc hại

a) Tạo lập, phát tán thông tin giả mạo, sai sự thật, vi phạm pháp luật trên hệ thống và nền tảng số của Trường.

b) Truy cập, phát tán hoặc sử dụng dịch vụ trực tuyến có nội dung độc hại, vi phạm pháp luật hoặc không phục vụ mục đích học tập, giảng dạy, nghiên cứu và quản lý của Trường.

c) Cản trở hoặc làm gián đoạn trái phép việc truyền tải thông tin trên các nền tảng số của Trường.

5. Xâm phạm dữ liệu cá nhân và tài nguyên thông tin

a) Thu thập, khai thác, sử dụng hoặc tiết lộ dữ liệu cá nhân của viên chức, người lao động, người học trái phép hoặc không đúng mục đích.

b) Chia sẻ dữ liệu, tài nguyên thông tin của Trường ra bên ngoài khi chưa được phép.

6. Các hành vi khác bị cấm theo Điều 8 Luật An ninh mạng và các quy định pháp luật liên quan.

Chương II

QUY ĐỊNH ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 6. Biện pháp đảm bảo an toàn thông tin và an ninh mạng

1. Trường thực hiện các biện pháp tổng thể nhằm bảo đảm an toàn thông tin và an ninh mạng đối với các hệ thống thông tin thuộc phạm vi quản lý, bao gồm biện pháp về kỹ thuật, quản trị và con người:

a) Biện pháp kỹ thuật gồm: thiết lập tường lửa, hệ thống phát hiện và ngăn chặn xâm nhập, cơ chế sao lưu và khôi phục dữ liệu định kỳ; mã hóa dữ liệu nhạy cảm, áp dụng cơ chế xác thực đa yếu tố, phân quyền truy cập theo vai trò; cập nhật, vá lỗi phần mềm, hệ điều hành và ứng dụng định kỳ.

b) Biện pháp quản trị gồm: ban hành và thực hiện các quy trình, quy định về sử dụng, vận hành, giám sát và bảo trì hệ thống thông tin; phân công rõ ràng trách nhiệm của các đơn vị, cá nhân trong việc bảo đảm an toàn thông tin; lưu trữ nhật ký truy cập, kiểm soát thay đổi cấu hình và đánh giá tính tuân thủ định kỳ.

c) Biện pháp về con người gồm: nâng cao nhận thức, tổ chức tập huấn định kỳ về an toàn thông tin cho viên chức, người lao động và người học; bảo mật tài khoản cá nhân, thư điện tử và các tài khoản truy cập khác.

2. Quản lý và đánh giá rủi ro: Viện Đổi mới sáng tạo và Chuyển đổi số chủ trì phối hợp với các đơn vị thực hiện đánh giá rủi ro an toàn thông tin định kỳ ít nhất một lần/năm hoặc theo hướng dẫn của cơ quan cấp trên; kết quả đánh giá được sử dụng để lập kế hoạch khắc phục, cải tiến hệ thống và báo cáo Lãnh đạo Trường và các cơ quan cấp trên khi có yêu cầu.

Điều 7. Đảm bảo an toàn thông tin tại phòng máy chủ và hệ thống mạng

1. Viện Đổi mới sáng tạo và Chuyển đổi số là đơn vị quản lý, vận hành hệ thống máy chủ (máy chủ vật lý, máy chủ ảo, máy chủ đám mây), hạ tầng mạng và dịch vụ Internet của Trường.

2. Viện Đổi mới sáng tạo và Chuyển đổi số thường xuyên kiểm tra và giám sát kết nối mạng Internet của các thiết bị đầu cuối; phát hiện, cảnh báo và ngăn chặn kịp thời các hành vi xâm nhập, tấn công bất hợp pháp.

3. Viện Đổi mới sáng tạo và Chuyển đổi số phối hợp với các đơn vị liên quan để xây dựng, đề xuất và triển khai các phương án bảo đảm an toàn cho hệ thống máy chủ, mạng và các hệ thống thông tin thuộc Trường.

4. Hệ thống thông tin phải ghi nhật ký truy cập và nhật ký sự kiện, bảo đảm lưu trữ tối thiểu 03 tháng; nhật ký phải được bảo vệ, kiểm tra định kỳ và chỉ cho phép truy cập bởi người có thẩm quyền.

5. Nghiêm cấm việc kết nối, cắm và sử dụng các thiết bị lưu trữ hoặc ngoại vi không được xác minh tính an toàn hoặc không có nguồn gốc rõ ràng vào máy tính, thiết bị công

nghệ thông tin của Trường. Trường hợp cần thiết phải được kiểm tra phần mềm độc hại và phê duyệt bởi Viện Đổi mới sáng tạo và Chuyển đổi số.

6. Phòng máy chủ là khu vực hạn chế, chỉ những cá nhân nhiệm vụ được phân công tiếp cận phòng máy chủ; được giám sát qua hệ thống camera và sổ nhật ký vào/ra phòng máy chủ.

7. Phòng máy chủ phải được trang bị đầy đủ giải pháp an toàn vật lý (nguồn điện dự phòng, hệ thống điều hòa, phòng cháy chữa cháy, chống sét, an toàn môi trường) để bảo đảm hoạt động ổn định, liên tục.

Điều 8. Đảm bảo an toàn thông tin đối với các hệ thống thông tin và cơ sở dữ liệu của Trường

1. Các 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 cá nhân thuộc Trường phải tắt thiết bị công nghệ thông tin, kịp thời thông báo với Viện Đổi mới sáng tạo và Chuyển đổi số để được hỗ trợ xử lý.

3. Các đơn vị được phân công quản lý, vận hành các thành phần hoặc mô-đun trong hệ thống thông tin dùng chung của Trường, ví dụ như: phân hệ quản lý đào tạo, phân hệ khảo thí, phân hệ kiểm định chất lượng,... có trách nhiệm phối hợp với Viện Đổi mới sáng tạo và Chuyển đổi số trong việc bảo đảm an toàn, duy trì tính sẵn sàng và cập nhật dữ liệu. Mỗi đơn vị chịu trách nhiệm về tính chính xác, đầy đủ và bảo mật thông tin thuộc phạm vi chức năng của mình trong hệ thống theo phân công chức năng nhiệm vụ của Trường. Viện Đổi mới sáng tạo và Chuyển đổi số chịu trách nhiệm quản lý hạ tầng, kỹ thuật, sao lưu, bảo trì và an toàn tổng thể của hệ thống.

4. Khi xây dựng mới, nâng cấp hoặc mở rộng hệ thống thông tin, đơn vị chủ trì phải phối hợp với Viện Đổi mới sáng tạo và Chuyển đổi số thực hiện quy trình thẩm định, kiểm thử, nghiệm thu và đưa vào sử dụng theo quy định của Trường. Quy trình thẩm định và nghiệm thu phải bảo đảm các yêu cầu tối thiểu về: bảo mật dữ liệu, phân quyền truy cập, khả năng sao lưu, phục hồi dữ liệu, và tính tương thích với các hệ thống thông tin hiện có. Viện Đổi mới sáng tạo và Chuyển đổi số hướng dẫn, hỗ trợ và xác nhận tính tuân thủ các tiêu

chuẩn kỹ thuật trước khi triển khai chính thức.

5. Đảm bảo hệ thống thông tin và cơ sở dữ liệu khi đưa vào khai thác phải vận hành thông suốt, an toàn và đáp ứng yêu cầu bảo mật.

6. Dữ liệu phải được sao lưu định kỳ (tối thiểu hàng tuần), có khả năng khôi phục khi xảy ra sự cố.

7. Dữ liệu mật, dữ liệu nhạy cảm phải được phân loại, gắn nhãn và áp dụng biện pháp mã hóa trong quá trình lưu trữ, truyền tải; việc quản lý khóa mã hóa và quyền truy cập chỉ được thực hiện bởi cá nhân, đơn vị được phân quyền.

8. Việc thu thập, lưu trữ, xử lý và chia sẻ thông tin cá nhân của giảng viên, viên chức, người lao động và người học phải tuân thủ quy định của Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân; chỉ được thực hiện khi có sự đồng ý của chủ thể dữ liệu và phục vụ mục đích công vụ của Trường.

9. Dữ liệu thuộc các hệ thống thông tin của Trường phải được lưu trữ tại hạ tầng máy chủ đặt tại phòng máy chủ/trung tâm dữ liệu của Trường hoặc trên nền tảng điện toán đám mây có chứng nhận bảo mật được phê duyệt.

10. Trường hợp đơn vị trực thuộc tự phát triển và đưa vào vận hành, khai thác phục vụ công tác chuyên môn của đơn vị cần phối hợp với Viện Đổi mới sáng tạo và Chuyển đổi số hỗ trợ thẩm định mức độ an toàn, tích hợp và giám sát tuân thủ các tiêu chuẩn kỹ thuật chung của Trường và tuân thủ Quy chế quản lý, vận hành, khai thác hạ tầng CNTT và hệ thống thông tin của Trường ban hành theo Quyết định số 1731/QĐ-ĐHTCM-QLTSCNTT ngày 03/6/2025.

Điều 9. 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. Mật khẩu phải có độ dài ít nhất 12 ký tự, bao gồm: chữ cái hoa và thường, ký tự số và ký tự đặc biệt. Việc thay đổi mật khẩu là bắt buộc khi có nghi ngờ mật khẩu bị lộ, khi có cảnh báo bảo mật hoặc sau sự cố an toàn thông tin. Trường hợp hệ thống yêu cầu thay đổi định kỳ, cá nhân không được tái sử dụng mật khẩu cũ.

2. Cá nhân có trách nhiệm bảo mật tài khoản, không chia sẻ thông tin truy cập cho người khác, đăng xuất sau khi sử dụng, và chịu trách nhiệm về mọi hành vi phát sinh từ tài khoản được cấp. Các tài khoản quản trị và tài khoản quan trọng phải áp dụng cơ chế xác thực đa yếu tố (Multi-Factor Authentication - MFA).

3. Việc truy cập vào hệ thống thông tin của Trường phải được kiểm soát chặt chẽ theo nguyên tắc phân quyền theo vai trò người dùng của cá nhân. Hệ thống phải ghi nhật ký truy cập, giám sát đăng nhập và phát hiện truy cập bất thường. Tài khoản truy cập phải được thu hồi khi không còn nhu cầu sử dụng hoặc khi người dùng không còn thuộc đối tượng được cấp quyền.

4. Việc điều chỉnh, tạm khóa hoặc thu hồi tài khoản phải được thực hiện kịp thời khi có thay đổi nhân sự, bao gồm:

a) Viên chức, người lao động chuyển công tác, nghỉ việc, nghỉ hưu, bị đình chỉ, bị kỷ luật, hoặc theo yêu cầu của đơn vị quản lý (do Phòng Tổ chức và Pháp chế thông báo);

b) Sinh viên, học viên, nghiên cứu sinh thôi học, tốt nghiệp hoặc bị đình chỉ (do đơn vị quản lý người học thông báo).

5. Viện Đổi mới sáng tạo và Chuyển đổi số thực hiện khóa, thu hồi tài khoản trong vòng 14 ngày kể từ ngày nhận được thông báo từ Phòng Tổ chức và Pháp chế hoặc các đơn vị quản lý người học. Đồng thời, Viện có quyền tạm khóa hoặc thu hồi tài khoản của người dùng khi phát hiện hành vi tấn công hệ thống hoặc bị nghi ngờ vi phạm quy chế, nhằm phục vụ công tác điều tra, xử lý sự cố an toàn thông tin và bảo đảm an toàn hệ thống chung.

6. Tài khoản thư điện tử (email) và các tài khoản truy cập hệ thống khác (Office 365, cổng thông tin nội bộ,…) được Trường cấp cho viên chức, người lao động và người học là tài sản thông tin thuộc quyền quản lý của Trường. Viện Đổi mới sáng tạo và Chuyển đổi số có trách nhiệm định kỳ rà soát tần suất sử dụng tài khoản thư điện tử của người dùng để bảo đảm an toàn và hiệu quả.

a) Trường hợp tài khoản thư điện tử không có hoạt động đăng nhập trong thời gian liên tục từ 90 (chín mươi) ngày trở lên, Viện Đổi mới sáng tạo và Chuyển đổi số có quyền tạm đình chỉ hoạt động tài khoản, gửi thông báo cảnh báo đến người sử dụng qua các kênh liên hệ khác (nếu có). Sau 30 (ba mươi) ngày kể từ khi đình chỉ mà không có yêu cầu kích hoạt hoặc sử dụng trở lại, tài khoản sẽ bị thu hồi, dữ liệu liên quan được lưu trữ thêm tối đa 60 (sáu mươi) ngày trước khi xóa vĩnh viễn theo quy trình kỹ thuật của Trường.

b) Việc đình chỉ, thu hồi và xóa dữ liệu tài khoản phải đảm bảo tuân thủ quy định của pháp luật về bảo vệ dữ liệu cá nhân và quy trình kỹ thuật của Trường.

c) Định kỳ ít nhất 03 tháng/lần, Viện Đổi mới sáng tạo và Chuyển đổi số rà soát, tự động tạm khóa các tài khoản email không hoạt động 90 ngày trở lên, lập biên bản và báo cáo kết quả rà soát cho Lãnh đạo Viện.

Điều 10. Đảm bảo an toàn thông tin trang thiết bị công nghệ thông tin cá nhân

1. Cá nhân chịu trách nhiệm bảo mật thiết bị và dữ liệu trên thiết bị của mình; phải thông báo ngay cho Viện Đổi mới sáng tạo và Chuyển đổi số khi thiết bị bị mất cắp, thất lạc hoặc có dấu hiệu bị xâm nhập.

2. Thiết bị cá nhân khi kết nối vào mạng của Trường phải đáp ứng yêu cầu an toàn: được cài đặt phần mềm chống mã độc bản quyền, cập nhật hệ điều hành và bản vá bảo mật thường xuyên.

3. Khi kết nối vào mạng của Trường, thiết bị cá nhân có thể được giám sát về lưu lượng và hành vi truy cập. Việc giám sát chỉ nhằm mục đích bảo đảm an toàn hệ thống, phòng chống mã độc, ngăn chặn truy cập trái phép và tuân thủ chính sách an toàn thông tin của Trường. Việc giám sát chỉ nhằm mục đích bảo đảm an toàn hệ thống, phòng chống tấn công và phát tán mã độc, tuân thủ quy định của pháp luật và không xâm phạm dữ liệu cá nhân thuần túy, nội dung riêng tư hoặc thông tin cá nhân của người sử dụng.

4. Thiết bị cá nhân sử dụng cho mục đích công việc phải đăng ký với Viện Đổi mới sáng tạo và Chuyển đổi số; việc truy cập vào hệ thống nội bộ của Trường được thực hiện thông qua kênh kết nối an toàn (VPN hoặc giải pháp tương đương).

5. Không lưu trữ dữ liệu mật hoặc dữ liệu nhạy cảm của Trường trên thiết bị cá nhân, trừ trường hợp được phép bằng văn bản và phải áp dụng biện pháp bảo mật theo hướng dẫn của Viện Đổi mới sáng tạo và Chuyển đổi số.

Điều 11. Ứng cứu sự cố an toàn hệ thống thông tin

1. Đội ứng cứu sự cố 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 và cơ sở dữ liệu thuộc Trường và phục hồi dữ liệu từ bản sao lưu gần nhất.

2. Đội ứng cứu sự cố an toàn thông tin mạng có trách nhiệm báo cáo, đề xuất phương án ứng cứu sự cố an toàn thông tin theo quy định của Trường, Bộ chủ quản và nhà nước; các sự cố nghiêm trọng phải báo cáo trong vòng 24 giờ kể từ khi phát hiện.

3. Đội ứng cứu sự cố an toàn thông tin mạng chủ trì, phối hợp với các đơn vị có liên quan tổ chức và tham gia diễn tập ứng cứu sự cố an toàn thông tin mạng định kỳ ít nhất một lần trong năm, bảo đảm phù hợp với kế hoạch của Trường và yêu cầu của bộ chủ quản và các cơ quan cấp trên; có thể kết hợp với kế hoạch diễn tập của bộ chủ quản hoặc thuê đơn vị bên ngoài tổ chức diễn tập thực chiến.

4. Đội ứng cứu sự cố an toàn thông tin mạng xây dựng kịch bản ứng phó sự cố an toàn thông tin hằng năm bao gồm các bước: phát hiện - cô lập - xử lý - phục hồi - đánh giá sau sự cố. Kịch bản phải được cập nhật định kỳ dựa trên kết quả kiểm tra, giám sát và đánh giá rủi ro. Sau mỗi sự cố gây mất an toàn, an ninh mạng, phải có báo cáo đánh giá, rút kinh nghiệm và cập nhật kịch bản ứng phó.

5. Các đơn vị, cá nhân liên quan có trách nhiệm phối hợp thực hiện ứng cứu sự cố theo phân công trong các kịch bản ứng phó và kế hoạch diễn tập ứng cứu an toàn thông tin mạng đã được phê duyệt, nhằm khôi phục hệ thống thông tin trong thời gian sớm nhất, hạn chế tối đa thiệt hại và rủi ro phát sinh.

6. Khi xảy ra sự cố nghiêm trọng vượt quá khả năng xử lý, Đội ứng cứu sự cố an toàn thông tin mạng, Viện Đổi mới sáng tạo và Chuyển đổi số phải kịp thời báo cáo và phối hợp với Bộ chủ quản, phối hợp với các cơ quan chức năng có thẩm quyền để thực hiện ứng cứu, khắc phục, bảo đảm khôi phục hệ thống theo đúng quy định pháp luật.

Chương III

TỔ CHỨC THỰC HIỆN

Điều 12. Trách nhiệm của các đơn vị thuộc và trực thuộc Trường

1. Phát hiện và báo cáo rủi ro

a) Các đơn vị, cá nhân khi phát hiện sự cố, rủi ro, lỗ hổng hoặc điểm yếu về an toàn thông tin trong quá trình quản lý, sử dụng hệ thống phải báo ngay cho Viện Đổi mới sáng tạo và Chuyển đổi số.

b) Thực hiện nghiêm túc các hướng dẫn, biện pháp khắc phục do Viện Đổi mới sáng tạo và Chuyển đổi số ban hành.

2. Tuân thủ và phối hợp

a) Triển khai, chấp hành các biện pháp bảo đảm an toàn thông tin theo Quy chế này và các văn bản chỉ đạo của Trường.

b) Phối hợp với Viện Đổi mới sáng tạo và Chuyển đổi số trong công tác giám sát, ứng cứu sự cố an toàn, an ninh mạng và khắc phục hậu quả.

c) Cá nhân, đơn vị vi phạm bị xử lý theo quy định pháp luật và Quy chế này.

3. Kết thúc sử dụng hệ thống thông tin và tài khoản

a) Khi có kế hoạch kết thúc sử dụng hệ thống thông tin, phải thực hiện sao lưu dữ liệu cần thiết và phối hợp với Viện Đổi mới sáng tạo và Chuyển đổi số để xóa, hủy dữ liệu nhạy cảm, thu hồi quyền truy cập.

b) Đối với viên chức, người lao động nghỉ việc hoặc sinh viên, học viên, nghiên cứu sinh kết thúc khóa học, đơn vị quản lý trực tiếp có trách nhiệm thông báo kịp thời cho Viện Đổi mới sáng tạo và Chuyển đổi số để thu hồi hoặc tạm khóa tài khoản.

4. Kiểm tra, giám sát và báo cáo

a) Định kỳ 6 tháng/lần, các đơn vị tổ chức tự kiểm tra, đánh giá việc thực hiện các quy định về bảo đảm an toàn, an ninh mạng trong phạm vi quản lý của mình bao gồm tối thiểu các nội dung sau: Quản lý và sử dụng tài khoản truy cập, mật khẩu và thiết bị công nghệ thông tin; Sao lưu, bảo mật dữ liệu và bảo vệ thông tin cá nhân; Tuân thủ quy định về cài đặt phần mềm, bảo mật thiết bị và kết nối mạng nội bộ; Báo cáo sự cố, rủi ro và tình hình khắc phục trong kỳ; Kết quả tuyên truyền, tập huấn, nâng cao nhận thức an toàn thông tin trong đơn vị. Kết quả tự kiểm tra phải được lưu trữ tại đơn vị tối thiểu 02 năm để phục vụ công tác kiểm tra, đánh giá định kỳ của Trường hoặc cơ quan quản lý cấp trên.

b) Gửi kết quả kiểm tra về Viện Đổi mới sáng tạo và Chuyển đổi số để tổng hợp, báo cáo Lãnh đạo Trường.

5. Đào tạo và nâng cao nhận thức

a) Tập huấn và hướng dẫn viên chức, người lao động và người học theo định kỳ hằng năm hoặc đột xuất theo yêu cầu.

b) Viên chức được giao phụ trách công nghệ thông tin và chuyển đổi số, an toàn an ninh mạng phải tham gia các khóa đào tạo chuyên sâu theo cấp độ hệ thống.

c) Tổ chức hoặc tham gia diễn tập ứng cứu sự cố an toàn thông tin mạng định kỳ ít nhất một lần trong năm, có thể kết hợp với kế hoạch diễn tập của Bộ, ngành và các cơ quan cấp trên hoặc thuê đơn vị bên ngoài.

6. Các đơn vị thuộc và trực thuộc Trường có trách nhiệm phối hợp thực hiện các biện pháp bảo đảm an toàn thông tin và an ninh mạng trong phạm vi quản lý, đồng thời chịu trách nhiệm về sao lưu dữ liệu, an toàn dữ liệu, truy cập và khai thác hệ thống thông tin của đơn vị mình.

Điều 13. Trách nhiệm của cá nhân

1. Tuân thủ nghiêm túc các quy định tại Quy chế này và các quy định pháp luật liên quan đến bảo đảm an toàn, an ninh mạng trong quá trình học tập, làm việc và sử dụng các hệ thống thông tin của Trường.

2. Bảo mật tài khoản, mật khẩu, thiết bị và dữ liệu được giao quản lý; hoặc sử dụng chung tài khoản, mật khẩu với bất kỳ cá nhân, tổ chức nào; không cài đặt hoặc sử dụng phần mềm không rõ nguồn phát hành, không được xác minh tính an toàn hoặc không có bản quyền hợp pháp; không tự ý sao chép, chia sẻ dữ liệu, thông tin của Trường ra ngoài khi chưa được phép của người có thẩm quyền.

3. Khi phát hiện nguy cơ hoặc sự cố an toàn thông tin (như lộ mật khẩu, mất thiết bị, email/tệp tin đáng ngờ, hành vi tấn công hoặc xâm nhập trái phép), cá nhân phải ngừng sử dụng thiết bị/tài khoản liên quan và báo cáo ngay cho Viện Đổi mới sáng tạo và Chuyển đổi số để được xử lý kịp thời.

4. Sử dụng thiết bị công nghệ thông tin theo đúng quy định: không cắm, kết nối các thiết bị lưu trữ hoặc ngoại vi không rõ nguồn gốc; thường xuyên cập nhật phần mềm bảo mật và hệ điều hành; thực hiện các biện pháp bảo vệ dữ liệu cá nhân, dữ liệu của Trường trong suốt quá trình sử dụng.

5. Người dùng có trách nhiệm bảo đảm an toàn thông tin trong quá trình giảng dạy,

nghiên cứu và sử dụng các thiết bị, dịch vụ của Trường; chỉ sử dụng tài khoản được cấp để truy cập, lưu trữ và chia sẻ học liệu, dữ liệu người học. Khi sử dụng thiết bị cá nhân (máy tính xách tay, điện thoại, USB,...) kết nối vào mạng nội bộ của Trường, người dùng phải đảm bảo thiết bị tuân thủ đầy đủ các quy định về an toàn thông tin. Thiết bị phải được cài đặt phần mềm chống mã độc, cập nhật hệ điều hành, trình duyệt và các ứng dụng lên phiên bản mới nhất; đồng thời người dùng không được cài đặt hoặc sử dụng phần mềm không rõ nguồn gốc, không được sao chép, lưu trữ dữ liệu nhạy cảm của Trường trên thiết bị cá nhân khi chưa được cho phép.

6. Tham gia đầy đủ các lớp bồi dưỡng, tập huấn, tuyên truyền, diễn tập ứng cứu sự cố an toàn thông tin do Trường hoặc các cơ quan, đơn vị có thẩm quyền tổ chức.

7. Chịu trách nhiệm trước pháp luật và Nhà trường về mọi hành vi vi phạm dẫn đến mất an toàn, an ninh mạng hoặc gây thiệt hại đến hệ thống, dữ liệu, uy tín và lợi ích hợp pháp của Trường.

Điều 14. Trách nhiệm của Viện Đổi mới sáng tạo và Chuyển đổi số

1. Xây dựng kế hoạch hằng năm về công tác an toàn, an ninh mạng, trình Lãnh đạo Trường phê duyệt và tổ chức triển khai; chủ động chuẩn bị phương án ứng phó với các sự cố có thể phát sinh và các thách thức từ không gian mạng.

2. Lập và triển khai kế hoạch đào tạo, bồi dưỡng nguồn nhân lực an toàn, an ninh mạng theo cấp độ; tổ chức tập huấn cơ bản cho toàn thể viên chức, người lao động và người học, đồng thời đào tạo chuyên sâu cho các viên chức được phụ trách công nghệ thông tin và chuyển đổi số.

3. Tham gia đóng góp ý kiến đối với các dự thảo văn bản quy phạm pháp luật, hướng dẫn về an toàn, an ninh mạng của các Bộ, ngành liên quan.

4. Tổ chức quét lỗ hổng bảo mật, đánh giá điểm yếu hệ thống thông tin định kỳ theo quy định (tối thiểu 03 tháng/lần) hoặc khi có yêu cầu; lập hồ sơ kết quả, lưu trữ và báo cáo Lãnh đạo Trường. Đối với các lỗ hổng có mức độ nghiêm trọng cao hoặc có nguy cơ bị khai thác ngay, Viện Đổi mới sáng tạo và Chuyển đổi số phải ưu tiên xử lý, khắc phục ngay sau khi phát hiện, đồng thời thông báo kịp thời cho các đơn vị liên quan để phối hợp triển khai biện pháp ngăn chặn, vá lỗi hoặc cô lập hệ thống (nếu có). Việc đánh giá và xử lý lỗ hổng phải được ghi nhận trong biên bản kỹ thuật và lưu giữ tối thiểu 12 tháng theo quy định lưu

trữ hồ sơ kỹ thuật.

5. Đề xuất, thiết lập, vận hành hệ thống giám sát an toàn thông tin bao gồm cả hệ thống SOC nội bộ hoặc thuê ngoài theo quy định, theo dõi nhật ký truy cập, nhật ký sự kiện, phát hiện và cảnh báo kịp thời các hành vi bất thường; ít nhất 06 tháng/lần báo cáo tình hình giám sát cho Lãnh đạo Trường và Bộ Tài chính; đồng thời thực hiện báo cáo đột xuất khi xảy ra sự cố nghiêm trọng hoặc khi có yêu cầu của cơ quan quản lý nhà nước.

6. Quản lý kỹ thuật các hệ thống công nghệ thông tin bao gồm quản lý cấu hình, phân quyền truy cập, sao lưu dữ liệu tập trung, vá lỗ hổng và cập nhật phần mềm/hệ thống kịp thời để bảo đảm an toàn, an ninh mạng theo cấp độ.

7. Hỗ trợ các tổ chức, đơn vị và cá nhân trong công tác bảo đảm an toàn, an ninh mạng; phối hợp ứng cứu sự cố và khắc phục khi cần thiết.

8. Chủ động phát hiện, báo cáo kịp thời các nguy cơ tiềm ẩn gây mất an toàn, an ninh mạng; phối hợp với bộ chủ quản và các cơ quan có thẩm quyền trong công tác ứng cứu, xử lý sự cố an toàn, an ninh mạng.

9. Phối hợp với Phòng Tổ chức và Pháp chế và các đơn vị liên quan trong việc tiếp nhận thông tin nhân sự (nghỉ việc, thôi việc, nghỉ hưu hoặc sinh viên, học viên, nghiên cứu sinh sau khi kết thúc khóa học, ra trường,…) để kịp thời điều chỉnh, tạm khóa hoặc thu hồi tài khoản người dùng theo quy định.

10. Định kỳ hằng năm, Viện Đổi mới sáng tạo và Chuyển đổi số tổ chức đánh giá việc tuân thủ Quy chế này; tổng hợp kết quả và đề xuất biện pháp cải tiến nhằm nâng cao hiệu quả quản lý an toàn thông tin, báo cáo Hiệu trưởng xem xét, chỉ đạo.

11. Viện Đổi mới sáng tạo và Chuyển đổi số là đầu mối báo cáo định kỳ kết quả đảm bảo an toàn, an ninh mạng cho Bộ chủ quản và các cơ quan cấp trên khi có yêu cầu.

12. Viện Đổi mới sáng tạo và Chuyển đổi số là đầu mối phối hợp với Phòng Tổ chức và Pháp chế để xử lý các vi phạm về an toàn, an ninh mạng theo quy định pháp luật.

Chương IV
ĐIỀU KHOẢN THI HÀNH

Điều 15. Điều khoản thi hành

1. Quy chế An toàn thông tin và An ninh mạng của Trường Đại học Tài chính - Marketing có hiệu lực kể từ ngày ký ban hành. Những nội dung chưa được quy định sẽ thực hiện theo quy định 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. Viện Đổi mới sáng tạo và Chuyển đổi số là đầu mối theo dõi, đôn đốc và tổng hợp tình hình triển khai để báo cáo Lãnh đạo Trường.

3. Việc bảo đảm an toàn thông tin và bảo mật dữ liệu trong hoạt động giảng dạy, học tập trực tuyến được thực hiện theo các hướng dẫn kỹ thuật có liên quan và Quy chế quản lý, vận hành, khai thác hạ tầng công nghệ thông tin và hệ thống thông tin của Trường ban hành theo Quyết định số 1731/QĐ-ĐHTCM-QLTSCNTT ngày 03/6/2025.

4. Quy chế này được phổ biến công khai đến toàn thể viên chức, người lao động và người học qua cổng thông tin điện tử và các kênh truyền thông nội bộ của Trường.

5. 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 bằng văn bản về Viện Đổi mới sáng tạo và Chuyển đổi số để tổng hợp, báo cáo Lãnh đạo Trường xem xét, phê duyệt việc sửa đổi, bổ sung. Việc rà soát, cập nhật Quy chế này được thực hiện định kỳ 02 năm/lần hoặc khi có thay đổi về chính sách, tiêu chuẩn bảo mật của Nhà nước./.

PHỤ LỤC 01

QUY TRÌNH AN TOÀN THÔNG TIN VÀ AN NINH MẠNG

(Ban hành kèm theo Quyết định số: 3684/QĐ-ĐHTCM ngày 10 tháng 11 năm 2025

của Hiệu trưởng Trường Đại học Tài chính - Marketing)

1. Quy trình đảm bảo an toàn thông tin tại phòng máy chủ

Bước	Đơn vị thực hiện	Lưu đồ thực hiện	Biểu mẫu/ Hồ sơ
1	Viện ĐMST&CĐS	Quản lý, vận hành hệ thống máy chủ/tiếp nhận yêu cầu truy cập máy chủ	BM/V.ĐMSTCĐS/21
2	Viện ĐMST&CĐS	Kiểm tra truy cập, vào/ra phòng máy chủ, an toàn vật lý Không	BM/V.ĐMSTCĐS/21
3	Viện ĐMST&CĐS	Đạt Giám sát và ghi sổ nhật ký vào/ra phòng máy chủ	Sổ nhật ký phòng máy chủ
4	Viện ĐMST&CĐS	Sao lưu theo định kỳ và phục hồi dữ liệu máy chủ khi có sự cố (nếu có)	
5	Viện ĐMST&CĐS	Báo cáo	BM/V.ĐMSTCĐS/21

Hình 1: *Lưu đồ quy trình đảm bảo an toàn thông tin tại phòng máy chủ.*

Mô tả quy trình:

Bước	Nội dung	Trách nhiệm đơn vị thực hiện	Trách nhiệm đơn vị phối hợp	Biểu mẫu thực hiện
1	Viện Đổi mới sáng tạo và Chuyển đổi số Quản lý, vận hành hệ thống máy chủ/tiếp nhận yêu cầu truy cập máy chủ	V.ĐMST&CĐS		BM/V.ĐMSTCĐS/21
2	Viện Đổi mới sáng tạo và Chuyển đổi số Kiểm tra truy cập hệ thống máy chủ, vào ra phòng máy chủ.	V.ĐMST&CĐS	Nhân viên, phòng ban, đơn vị	BM/V.ĐMSTCĐS/21
3	Viện Đổi mới sáng tạo và Chuyển đổi số Giám sát và ghi sổ nhật ký vào/ra phòng máy chủ.	V.ĐMST&CĐS		Ghi Sổ nhật ký
4	Viện Đổi mới sáng tạo và Chuyển đổi số Sao lưu theo định kỳ và phục hồi dữ liệu máy chủ khi có sự cố (nếu có)	V.ĐMST&CĐS		
5	Viện Đổi mới sáng tạo và Chuyển đổi số báo cáo	V.ĐMST&CĐS		BM/V.ĐMSTCĐS/21

Biểu mẫu:

STT	Nội dung	Mã hóa biểu mẫu	Nơi lưu	Thời gian lưu
1	Biểu mẫu đăng ký truy cập hệ thống máy chủ	BM/V.ĐMSTCĐS/21	V.ĐMSTCĐS	05 năm
2	Mẫu biên bản kiểm tra truy cập hệ thống máy chủ	BM/V.ĐMSTCĐS/21	V.ĐMSTCĐS	05 năm
3	Mẫu báo cáo hệ thống máy chủ	BM/V.ĐMSTCĐS/21	V.ĐMSTCĐS	05 năm
4	Sổ nhật ký phòng máy chủ			

2. Quy trình đảm bảo an toàn thông tin hệ thống mạng và kết nối Internet

Bước	Đơn vị thực hiện	Lưu đồ thực hiện	Biểu mẫu/ Hồ sơ
1	Viện ĐMST&CĐS	Quản lý, vận hành hạ tầng mạng/tiếp nhận yêu cầu	BM/V.ĐMSTCĐS/22
2	Viện ĐMST&CĐS	Kiểm tra tình trạng hoạt động của hệ thống mạng Đạt	BM/V.ĐMSTCĐS/22
3	Viện ĐMST&CĐS	Không đạt Xử lý và khắc phục sự cố	
4	Viện ĐMST&CĐS	Kiểm tra, đánh giá sau khi xử lý Không đạt Đạt	BM/V.ĐMSTCĐS/22
5	Viện ĐMST&CĐS	Quản trị và vận hành hệ thống mạng an toàn	
6	Viện ĐMST&CĐS	Báo cáo	BM/V.ĐMSTCĐS/22

Hình 2: *Lưu đồ quy trình đảm bảo an toàn thông tin hệ thống mạng và kết nối Internet.*

Mô tả quy trình:

Bước	Nội dung	Trách nhiệm đơn vị thực hiện	Trách nhiệm đơn vị phối hợp	Biểu mẫu thực hiện
1	Viện ĐMST&CĐS quản lý, vận hành hạ tầng mạng/tiếp nhận yêu cầu	V.ĐMST&CĐS		BM/V.ĐMSTCĐS/22
2	Viện ĐMST&CĐS kiểm tra tình trạng hoạt động của hệ thống mạng	V.ĐMST&CĐS		BM/V.ĐMSTCĐS/22
3	Viện ĐMST&CĐS xử lý và khắc phục sự cố	V.ĐMST&CĐS	Nhân viên, đơn vị	
4	Viện ĐMST&CĐS kiểm tra, đánh giá sau khi xử lý	V.ĐMST&CĐS		BM/V.ĐMSTCĐS/22
5	Viện ĐMST&CĐS quản trị và vận hành hệ thống mạng an toàn	V.ĐMST&CĐS		
6	Viện ĐMST&CĐS báo cáo hệ thống mạng và kết nối Internet	V.ĐMST&CĐS		BM/V.ĐMSTCĐS/22

Biểu mẫu:

STT	Nội dung	Mã hóa biểu mẫu	Nơi lưu	Thời gian lưu
1	Biểu mẫu tiếp nhận yêu cầu kiểm tra mạng và đường truyền Internet.	BM/V.ĐMSTCĐS/22	V.ĐMSTCĐS	05 năm
2	Mẫu biên bản kiểm tra tình trạng hoạt động hệ thống mạng và kết nối Internet	BM/V.ĐMSTCĐS/22	V.ĐMSTCĐS	05 năm
3	Mẫu báo cáo	BM/V.ĐMSTCĐS/22	V.ĐMSTCĐS	05 năm

3. Quy trình đảm bảo an toàn thông tin quản lý và sử dụng tài khoản truy cập các hệ thống thông tin

Bước	Đơn vị thực hiện	Lưu đồ thực hiện	Biểu mẫu/ Hồ sơ
1	Viện ĐMST&CĐS	Tiếp nhận yêu cầu xử lý	BM/V.ĐMSTCĐS/23
2	Viện ĐMST&CĐS	Kiểm tra, xác thức, bảo mật tài khoản Không đạt	
3	Viện ĐMST&CĐS	Đạt Thực hiện xử lý	
4	Viện ĐMST&CĐS	Không đạt Kiểm tra, sau xử lý	BM/V.ĐMSTCĐS/23
5	Viện ĐMST&CĐS	Đạt Thông báo	BM/V.ĐMSTCĐS/23
6	Nhân viên, phòng ban, đơn vị	Tài khoản sử dụng theo chức năng được giao	

Hình 3: *Lưu đồ quy trình đảm bảo an toàn thông tin quản lý và sử dụng tài khoản truy cập các hệ thống thông tin*

Mô tả quy trình:

Bước	Nội dung	Trách nhiệm đơn vị thực hiện	Trách nhiệm đơn vị phối hợp	Biểu mẫu thực hiện
1	Viện ĐMST & CĐS tiếp nhận yêu cầu phát sinh tài khoản.	V.ĐMST&CĐS	Nhân viên, phòng ban, đơn vị	BM/V.ĐMSTCĐS/23
2	Viện ĐMST & CĐS kiểm tra, xác thực, bảo mật tài khoản.	V.ĐMST&CĐS	Nhân viên, phòng ban,đơn vị	
3	Viện Đổi mới sáng tạo và Chuyển đổi số thực hiện xử lý.	V.ĐMST&CĐS	Nhân viên, phòng ban, đơn vị	
4	Viện ĐMST & CĐS kiểm tra, sau xử lý	V.ĐMST&CĐS	Nhân viên, phòng ban, đơn vị	BM/V.ĐMSTCĐS/23
5	Viện ĐMST & CĐS định kỳ rà soát và tự động tạm khóa các tài khoản email không hoạt động 90 ngày trở lên; báo cáo kết quả cho Lãnh đạo Viện và thông báo cảnh báo đến người dùng	V.ĐMST&CĐS	Nhân viên, phòng ban, đơn vị	BM/V.ĐMSTCĐS/23
6	Nhân viên, phòng ban, đơn vị tiếp tục được sử dụng theo chức năng được cấp	Nhân viên, phòng ban, đơn vị	V.ĐMST&CĐS	

Biểu mẫu:

STT	Nội dung	Mã hóa biểu mẫu	Nơi lưu	Thời gian lưu
1	Biểu mẫu tiếp nhận yêu cầu phát sinh tài khoản	BM/V.ĐMSTCĐS/23	V.ĐMSTCĐS	05 năm
2	Mẫu biên bản kiểm tra, kiểm soát tài khoản	BM/V.ĐMSTCĐS/23	V.ĐMSTCĐS	05 năm
3	Mẫu thông báo hỗ trợ, thu hồi tài khoản	BM/V.ĐMSTCĐS/23	V.ĐMSTCĐS	05 năm

4. Quy trình đảm bảo an toàn thông tin trang thiết bị công nghệ thông tin cá nhân truy cập hệ thống máy chủ

Bước	Đơn vị thực hiện	Lưu đồ thực hiện	Biểu mẫu/ Hồ sơ
1	Cá nhân, đơn vị, tổ chức	Đăng ký thiết bị truy cập hệ thống máy chủ (vật lý, cloud server) và hệ thống thông tin	BM/V.ĐMSTCĐS/24
2	Viện ĐMST&CĐS	Kiểm tra hệ điều hành, phần mềm diệt virus trên thiết bị cá nhân Không đạt	BM/V.ĐMSTCĐS/24
3	Viện ĐMST&CĐS	Đạt Cấp quyền truy cập hệ thống máy chủ (vật lý, cloud server) và hệ thống thông tin	
4	Viện ĐMST&CĐS	Thực hiện, giám sát, xử lý	
5	Cá nhân, đơn vị, tổ chức, Viện ĐMST&CĐS	Giám sát sự cố phát sinh Không đạt Đạt	BM/V.ĐMSTCĐS/24
6	Viện ĐMST&CĐS	Báo cáo	BM/V.ĐMSTCĐS/24

Hình 4: *Lưu đồ quy trình đảm bảo an toàn thông tin trang thiết bị công nghệ thông tin cá nhân truy cập hệ thống máy chủ*

Mô tả quy trình:

Bước	Nội dung	Trách nhiệm đơn vị thực hiện	Trách nhiệm đơn vị phối hợp	Biểu mẫu thực hiện
1	Thiết bị cá nhân sử dụng cho mục đích công việc phải đăng ký với Viện ĐMST&CĐS; việc truy cập truy cập hệ thống máy chủ (vật lý, cloud server) và hệ thống thông tin	Cá nhân, đơn vị, tổ chức	V.ĐMSTCĐS	BM/V.ĐMSTCĐS/24
2	Viện ĐMST&CĐS thực hiện Kiểm tra hệ điều hành, phần mềm diệt virus trên thiết bị cá nhân.	V.ĐMST&CĐS	Cá nhân, đơn vị, tổ chức	BM/V.ĐMSTCĐS/24
3	Viện ĐMST&CĐS cấp quyền truy cập hệ thống máy chủ (vật lý, cloud server) và hệ thống thông tin.	V.ĐMST&CĐS	Cá nhân, đơn vị, tổ chức	
4	Viện ĐMST&CĐS thực hiện, giám sát, xử lý.	V.ĐMST&CĐS	Cá nhân, đơn vị, tổ chức	
5	Thông báo Viện ĐMST&CĐS giám sát sự cố phát sinh	V.ĐMST&CĐS		BM/V.ĐMSTCĐS/24
6	Thực hiện báo cáo hoàn thành công việc	V.ĐMST&CĐS		BM/V.ĐMSTCĐS/24

Biểu mẫu:

STT	Nội dung	Mã hóa biểu mẫu	Nơi lưu	Thời gian lưu
1	Biểu mẫu tiếp nhận đăng ký thiết bị truy cập hệ thống máy chủ	BM/V.ĐMSTCĐS/24	V.ĐMSTCĐS	05 năm
2	Mẫu biên bản kiểm tra thiết bị công nghệ thông tin cá nhân truy cập hệ thống máy chủ	BM/V.ĐMSTCĐS/24	V.ĐMSTCĐS	05 năm
3	Mẫu thông báo sự cố bất thường truy cập hệ thống máy chủ	BM/V.ĐMSTCĐS/24	V.ĐMSTCĐS	05 năm
4	Mẫu báo cáo hoàn thành công việc	BM/V.ĐMSTCĐS/24	V.ĐMSTCĐS	05 năm

5. Quy trình ứng phó sự cố an toàn thông tin mạng

Bước	Đơn vị thực hiện	Lưu đồ thực hiện	Biểu mẫu/ Hồ sơ
1	Đơn vị thuộc trường	Tiếp nhận yêu cầu	BM/V.ĐMSTCĐS/25
2	Viện ĐMST&CĐS	Đánh giá và phân loại sự cố	
3	Viện ĐMST&CĐS	Phân tích và đề xuất phương án	BM/V.ĐMSTCĐS/25
4	Lãnh đạo Viện ĐMST&CĐS	Xem xét? (Không duyệt / Duyệt)	
5	Ban giám hiệu phụ trách	Phê duyệt phương án (Duyệt)	BM/V.ĐMSTCĐS/25
6	Viện ĐMST&CĐS K.KHDL	Thực hiện, ứng cứu sự cố an toàn thông tin mạng	BM/V.ĐMSTCĐS/25
7	Viện ĐMST&CĐS	Kiểm tra đánh giá hệ thống sau khi khắc phục (Kiểm tra / Không đáp ứng)	BM/V.ĐMSTCĐS/25
8	Viện ĐMST&CĐS K.KHDL	Báo cáo và rút kinh nghiệm (Đáp ứng)	BM/V.ĐMSTCĐS/25
9	Viện ĐMST&CĐS	Lưu báo cáo	BM/V.ĐMSTCĐS/25

Hình 5: *Lưu đồ quy trình ứng phó sự cố an toàn thông tin mạng*

Mô tả quy trình:

Bước	Nội dung	Trách nhiệm đơn vị thực hiện	Trách nhiệm đơn vị phối hợp	Biểu mẫu thực hiện
1	Tiếp nhận yêu cầu từ đơn vị thuộc Trường	V.ĐMST&CĐS	Các đơn vị thuộc Trường	BM/V.ĐMSTCĐS/25
2	Đánh giá và phân loại sự cố an toàn thông tin mạng để xây dựng kế hoạch ứng phó	V.ĐMST&CĐS	Các đơn vị thuộc Trường	BM/V.ĐMSTCĐS/25
3	Phân tích nguyên nhân và đề xuất phương án giám sát hệ thống và xử lý sự cố	V.ĐMST&CĐS	Các đơn vị thuộc Trường	BM/V.ĐMSTCĐS/25
4	Lãnh đạo Phòng Quản lý tài sản và Công nghệ thông tin và lãnh đạo Khoa Khoa học dữ liệu xem xét và duyệt phương án đề xuất	V.ĐMST&CĐS, K.KHDL		
5	Trình BGH phê duyệt phương án	V.ĐMST&CĐS	Các đơn vị thuộc Trường	BM/V.ĐMSTCĐS/25
6	Thực hiện phương án ứng cứu sự cố an toàn thông tin mạng	V.ĐMST&CĐS, K.KHDL	Các đơn vị thuộc Trường, Các đơn vị ngoài Trường (nếu có)	BM/V.ĐMSTCĐS/25
7	Kiểm tra hệ thống trước khi đưa vào vận hành và khai thác trở lại	V.ĐMST&CĐS, K.KHDL	Các đơn vị thuộc Trường, Các đơn vị ngoài Trường (nếu có)	BM/V.ĐMSTCĐS/25
8	Báo cáo và rút kinh nghiệm, đánh giá quy trình và cập nhật biện pháp phòng ngừa	V.ĐMST&CĐS, K.KHDL	Các đơn vị thuộc Trường, Các đơn vị ngoài Trường (nếu có)	BM/V.ĐMSTCĐS/25
9	Lưu báo cáo	V.ĐMST&CĐS		BM/V.ĐMSTCĐS/25

Biểu mẫu:

STT	Nội dung	Mã hóa biểu mẫu	Nơi lưu	Thời gian lưu
1	Biểu mẫu quy trình ứng phó sự cố an toàn thông tin mạng	BM/V.ĐMSTCĐS/25	V.ĐMSTCĐS	05 năm

PHỤ LỤC 02
BIỂU MẪU AN TOÀN THÔNG TIN VÀ AN NINH MẠNG

BM/V.ĐMSTCĐS/21

TRƯỜNG ĐẠI HỌC
TÀI CHÍNH - MARKETING
VIỆN ĐỔI MỚI SÁNG TẠO
VÀ CHUYỂN ĐỔI SỐ

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

Thành phố Hồ Chí Minh, ngày ... tháng ... năm .....

BIÊN BẢN ĐĂNG KÝ
TRUY CẬP HỆ THỐNG MÁY CHỦ

1. Họ và tên người truy cập: .....
2. Đơn vị công tác: .....
3. Ngày đề xuất: ...../...../.....
4. Thiết bị đăng ký:.....
5. Nội dung công việc truy cập máy chủ:

.....

.....

.....

.....

.....

Người truy cập	**Người tiếp nhận**	**VIỆN ĐMSTCĐS**
(Ký, ghi đầy đủ họ tên)	*(Ký, ghi đầy đủ họ tên)*	*(Ký, ghi đầy đủ họ tên)*

Nơi nhận:
- Lãnh đạo Viện ĐMSTCĐS;
- Lưu: ĐMSTCĐS.

BM/V.ĐMSTCĐS/21

TRƯỜNG ĐẠI HỌC
TÀI CHÍNH - MARKETING
VIỆN ĐỔI MỚI SÁNG TẠO VÀ CHUYỂN ĐỔI SỐ

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

Thành phố Hồ Chí Minh, ngày ... tháng ... năm .....

BIÊN BẢN KIỂM TRA
TRUY CẬP HỆ THỐNG MÁY CHỦ

1. Nội dung kiểm tra *(Ghi chi tiết tên các thiết bị/phần mềm)*:.....

.....

.....

.....

.....

.....

.....

.....

.....

2. Báo cáo kết quả sau kiểm tra:

.....

.....

.....

3. Kiến nghị *(nếu có)*:

.....

.....

.....

NGƯỜI BÁO CÁO **VIỆN ĐMSTCĐS**

Nơi nhận:
- Lãnh đạo Viện ĐMSTCĐS;
- Lưu: ĐMSTCĐS.

BM/V.ĐMSTCĐS/21

TRƯỜNG ĐẠI HỌC
TÀI CHÍNH - MARKETING
VIỆN ĐỔI MỚI SÁNG TẠO
VÀ CHUYỂN ĐỔI SỐ

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

Thành phố Hồ Chí Minh, ngày ... tháng ... năm .....

BÁO CÁO

(Về .....)

1. Người thực hiện:

STT	Họ và tên	Đơn vị	Công việc
1			
2			

2. Báo cáo chi tiết: *(tất cả hệ thống thông tin liên quan)*:

- Hệ thống máy chủ: .....

+ Trước sự cố nếu có: .....
.....

+ Sau sự cố: .....
.....

+ Đánh giá: .....

- Hệ thống phần mềm: .....

+ Trước sự cố nếu có: .....
.....

+ Sau sự cố: .....

+ Đánh giá: .....

3. Giải pháp/ đề xuất *(quan trọng nếu có)*: .....
.....

NHÂN VIÊN QUẢN LÝ
PHÒNG MÁY CHỦ

VIỆN ĐMSTCĐS

Nơi nhận:
- Lãnh đạo Viện ĐMSTCĐS;
- Lưu: ĐMSTCĐS.

BM/V.ĐMSTCĐS/22

TRƯỜNG ĐẠI HỌC
TÀI CHÍNH - MARKETING
VIỆN ĐỔI MỚI SÁNG TẠO
VÀ CHUYỂN ĐỔI SỐ

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

Thành phố Hồ Chí Minh, ngày ... tháng ... năm .....

BIÊN BẢN TIẾP NHẬN YÊU CẦU KIỂM TRA MẠNG VÀ ĐƯỜNG TRUYỀN INTERNET

1. Họ và tên người yêu cầu: .....

2. Đơn vị công tác: .....

3. Địa điểm kiểm tra: *(Liệt kê một hoặc nhiều cơ sở)*

.....

.....

4. Hệ thống mạng: *(Liệt kê các hệ thống mạng)*

.....

.....

5. Nội dung kiểm tra: *(nếu có hoặc đính kèm văn bản)*

.....

.....

.....

.....

.....

Viện ĐMSTCĐS	**Người yêu cầu**	**Người tiếp nhận**
Phê duyệt:	*(Ký, ghi đầy đủ họ tên)*	*(Ký, ghi đầy đủ họ tên)*
(Ký, ghi đầy đủ họ tên)		

Mã tiếp nhận: .....

Nơi nhận:
- Lãnh đạo Viện ĐMSTCĐS;
- Lưu: ĐMSTCĐS.

BM/V.ĐMSTCĐS/22

TRƯỜNG ĐẠI HỌC
TÀI CHÍNH - MARKETING
VIỆN ĐỔI MỚI SÁNG TẠO
VÀ CHUYỂN ĐỔI SỐ

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

Thành phố Hồ Chí Minh, ngày ... tháng ... năm .....

BÁO CÁO KIỂM TRA TÌNH TRẠNG HOẠT ĐỘNG HỆ THỐNG MẠNG VÀ KẾT NỐI INTERNET

1. Hệ thống mạng cơ sở: .....

.....

2. Nhân viên thực hiện: .....

3. Nhân viên phối hợp: .....

4. Chi tiết thực hiện:

STT	Nội dung kiểm tra	Kết quả
1	Kiểm tra tốc độ mạng Lan	
2	Kiểm tra tốc độ Internet	
3		
...		

5. Báo cáo chi tiết: *(Đính kèm biên bản của nhà cung cấp dịch vụ)*

.....

.....

6. Kiến nghị:

.....

.....

VIỆN ĐMSTCĐS
(Ký, ghi đầy đủ họ tên)

NGƯỜI BÁO CÁO
(Ký, ghi đầy đủ họ tên)

Nơi nhận:
- Lãnh đạo Viện ĐMSTCĐS;
- Lưu: ĐMSTCĐS.

BM/V.ĐMSTCĐS/22

TRƯỜNG ĐẠI HỌC
TÀI CHÍNH - MARKETING
VIỆN ĐỔI MỚI SÁNG TẠO
VÀ CHUYỂN ĐỔI SỐ

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

Thành phố Hồ Chí Minh, ngày ... tháng ... năm .....

BÁO CÁO
(Về.....)

1. Mã tiếp nhận: .....

2. Hệ thống mạng:

.....

.....

3. Chi tiết thực hiện:

STT	Họ và tên	Nội dung công việc
1	Trần Văn A	- 09 giờ ngày xx/xx/xxxx: Bảo trì hệ thống mạng và Internet cơ sở 27 Tân Mỹ - 14 giờ ngày xx/xx/xxxx: Bảo trì hệ thống mạng và Internet cơ sở Long Trường
2	Nguyễn Thị B	- 09 giờ ngày xx/xx/xxxx: Bảo trì hệ thống mạng và Internet Trụ sở 778 Nguyễn Kiệm
...		

4. Báo cáo chi tiết: *(Đính kèm biên bản của nhà cung cấp dịch vụ nếu có)*

.....

.....

5. Kiến nghị:

.....

.....

VIỆN ĐMSTCĐS
(Ký, ghi đầy đủ họ tên)

NGƯỜI BÁO CÁO
(Ký, ghi đầy đủ họ tên)

Nơi nhận:
- Lãnh đạo Viện ĐMSTCĐS;
- Lưu: ĐMSTCĐS.

BM/V.ĐMSTCĐS/23

TRƯỜNG ĐẠI HỌC
TÀI CHÍNH - MARKETING
VIỆN ĐỔI MỚI SÁNG TẠO
VÀ CHUYỂN ĐỔI SỐ

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

Thành phố Hồ Chí Minh, ngày ... tháng ... năm ... ...

BIÊN BẢN TIẾP NHẬN
YÊU CẦU PHÁT SINH TÀI KHOẢN

Mã yêu cầu: .....

Thời gian tiếp nhận ..... giờ ....., .../...../20.....

Kênh tiếp nhận ☐ Email ☐ Zalo ☐ Điện thoại ☐ Trực tiếp

Người tiếp nhận: .....

1. Người yêu cầu

Họ và tên: .....

Mã số/Đơn vị: .....

Liên hệ Email/ĐT: .....

2. Hệ thống và loại yêu cầu:

Hệ thống: ☐ Email/Workspace ☐ Portal ☐ Khác: .....

Loại: ☐ Cấp mới ☐ Đặt lại MK ☐ Mở khóa ☐ Điều chỉnh quyền ☐ Thu hồi

3. Mô tả ngắn gọn:

.....

4. Xử lý và kết quả:

Người xử lý: ..... Thời gian: ...../...../20....

Thao tác: ☐ Tạo TK ☐ Đặt lại MK ☐ Mở khóa ☐ Điều chỉnh quyền ☐ Khác: .....

Ghi chú/Kết quả: .....

Viện ĐMSTCĐS	**Người yêu cầu**	**Người tiếp nhận**
Phê duyệt:	*(Ký, ghi đầy đủ họ tên)*	*(Ký, ghi đầy đủ họ tên)*
(Ký, ghi đầy đủ họ tên)		

Nơi nhận:
- Lãnh đạo Viện ĐMSTCĐS;
- Lưu: ĐMSTCĐS.

BM/V.ĐMSTCĐS/23

TRƯỜNG ĐẠI HỌC
TÀI CHÍNH - MARKETING
VIỆN ĐỔI MỚI SÁNG TẠO
VÀ CHUYỂN ĐỔI SỐ

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

Thành phố Hồ Chí Minh, ngày ... tháng ... năm .....

BIÊN BẢN KIỂM TRA, KIỂM SOÁT TÀI KHOẢN

Thời gian lập biên bản: ..... giờ ..... phút, ngày ..... tháng ..... năm .....
Địa điểm: .....

I. Thành phần tham gia kiểm tra:

1. Ông/Bà: .....Chức vụ: .....

Thông tin thiết bị cá nhân:
- Họ và tên chủ thiết bị: .....
- Đơn vị công tác: .....
- Loại thiết bị: □ Laptop □ Điện thoại □ Máy tính bảng □ Khác: .....
- Nhãn hiệu – Model: ..... Hệ điều hành:.....
- Địa chỉ MAC: ..... Địa chỉ IP *(nếu có)*:.....
- Phần mềm truy cập hệ thống: .....
- Tài khoản sử dụng: .....

II. Nội dung kiểm tra:

STT	Hạng mục kiểm tra	Kết quả kiểm tra	Ghi chú
1	Thiết bị có cài phần mềm diệt virus	□ Đạt □ Không đạt	
2	Thiết bị đã cập nhật hệ điều hành mới nhất	□ Đạt □ Không đạt	
3	Thiết bị có mã hóa dữ liệu	□ Có □ Không	
4	Thiết bị có sử dụng VPN khi truy cập	□ Có □ Không	
5	Thiết bị có lưu thông tin nhạy cảm	□ Có □ Không	
6	Thiết bị có tuân thủ chính sách truy cập	□ Có □ Không	

Kết luận:
.....
.....
Ý kiến của chủ thiết bị:
.....
.....

ĐẠI DIỆN ĐƠN VỊ KIỂM TRA
(Ký, ghi đầy đủ họ tên)

CHỦ THIẾT BỊ
(Ký, ghi đầy đủ họ tên)

BM/V.ĐMSTCĐS/23

TRƯỜNG ĐẠI HỌC
TÀI CHÍNH - MARKETING
VIỆN ĐỔI MỚI SÁNG TẠO
VÀ CHUYỂN ĐỔI SỐ

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

Thành phố Hồ Chí Minh, ngày ... tháng ... năm .....

BIÊN BẢN
THÔNG BÁO HỖ TRỢ, THU HỒI TÀI KHOẢN

Thời gian lập biên bản: ..... giờ ..... phút, ngày ..... tháng ..... năm .....

Địa điểm: .....

I. Thành phần tham dự

1. Ông/Bà: [Họ tên người lập biên bản]:.....
   Chức vụ:.....
2. Ông/Bà: [Họ tên người sử dụng tài khoản]:.....
   Chức vụ: [Chức vụ]:.....
3. Các bên liên quan khác (nếu có): .....

II. Nội dung:

1. Thông báo cấp tài khoản truy cập:

- Tài khoản: [Tên tài khoản] .....
- Hệ thống: [Tên hệ thống thông tin] .....
- Quyền truy cập: [Mô tả quyền hạn].....
- Thời gian hiệu lực: từ ngày …./…../……. đến ngày …./…../……

2. Hỗ trợ sử dụng:

- Hướng dẫn đăng nhập, sử dụng hệ thống (nếu có):.....
- Cung cấp tài liệu hướng dẫn (nếu có):.....
- Liên hệ hỗ trợ kỹ thuật: [Thông tin liên hệ] .....

3. Thu hồi tài khoản:

- Lý do thu hồi: [Ví dụ: nghỉ việc, chuyển công tác, vi phạm quy định,…].....
- Thời điểm thu hồi: … giờ … phút, ngày … tháng … năm .....
- Biện pháp xử lý dữ liệu liên quan: [Ví dụ: lưu trữ, chuyển giao,…].....

III. Cam kết và xác nhận:

Các bên xác nhận đã hiểu rõ nội dung biên bản và cam kết thực hiện đúng quy định về bảo mật thông tin và sử dụng hệ thống.

IV. Chữ ký xác nhận

Người lập biên bản: *(Ký, ghi rõ họ tên)*.....

Người sử dụng tài khoản: *(Ký, ghi rõ họ tên)*.....

Đại diện đơn vị quản lý hệ thống: *(Ký, ghi rõ họ tên)*.....

BM/V.ĐMSTCĐS/24

TRƯỜNG ĐẠI HỌC
TÀI CHÍNH - MARKETING
VIỆN ĐỔI MỚI SÁNG TẠO
VÀ CHUYỂN ĐỔI SỐ

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

Thành phố Hồ Chí Minh, ngày ... tháng ... năm .....

BIÊN BẢN TIẾP NHẬN
ĐĂNG KÝ THIẾT BỊ TRUY CẬP HỆ THỐNG MÁY CHỦ

1. Họ và tên người đề xuất: .....
2. Đơn vị công tác: .....
3. Ngày đề xuất: ...../...../.....
4. Thiết bị đăng ký:.....
5. Nội dung công việc truy cập máy chủ:

.....

.....

.....

.....

.....

.....

.....

.....

Người đề xuất	**Người tiếp nhận**	**VIỆN ĐMSTCĐS**
(Ký, ghi đầy đủ họ tên)	*(Ký, ghi đầy đủ họ tên)*	*(Ký, ghi đầy đủ họ tên)*

Nơi nhận:
- Lãnh đạo Viện ĐMSTCĐS;
- Lưu: ĐMSTCĐS.

BM/V.ĐMSTCĐS/24

TRƯỜNG ĐẠI HỌC
TÀI CHÍNH - MARKETING
VIỆN ĐỔI MỚI SÁNG TẠO
VÀ CHUYỂN ĐỔI SỐ

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

Thành phố Hồ Chí Minh, ngày ... tháng ... năm .....

BIÊN BẢN KIỂM TRA THIẾT BỊ CÔNG NGHỆ THÔNG TIN CÁ NHÂN TRUY CẬP HỆ THỐNG MÁY CHỦ

Thời gian lập biên bản: ..... giờ ..... phút, ngày ..... tháng ..... năm .....
Địa điểm: .....

I. Thành phần tham gia kiểm tra:

1. Ông/Bà: .....Chức vụ: .....

Thông tin thiết bị cá nhân:

- Họ và tên chủ thiết bị: .....
- Đơn vị công tác: .....
- Loại thiết bị: □ Laptop □ Điện thoại □ Máy tính bảng □ Khác: .....
- Nhãn hiệu – Model: ..... Hệ điều hành:.....
- Địa chỉ MAC: ..... Địa chỉ IP *(nếu có)*:.....
- Phần mềm truy cập hệ thống: .....
- Tài khoản sử dụng: .....

II. Nội dung kiểm tra:

STT	Hạng mục kiểm tra	Kết quả kiểm tra	Ghi chú
1	Thiết bị có cài phần mềm diệt virus	□ Đạt □ Không đạt	
2	Thiết bị đã cập nhật hệ điều hành mới nhất	□ Đạt □ Không đạt	
3	Thiết bị có mã hóa dữ liệu	□ Có □ Không	
4	Thiết bị có sử dụng VPN khi truy cập	□ Có □ Không	
5	Thiết bị có lưu thông tin nhạy cảm	□ Có □ Không	
6	Thiết bị có tuân thủ chính sách truy cập	□ Có □ Không	

Kết luận:
.....
.....
Ý kiến của chủ thiết bị:
.....
.....

ĐẠI DIỆN ĐƠN VỊ KIỂM TRA
(Ký, ghi đầy đủ họ tên)

CHỦ THIẾT BỊ
(Ký, ghi đầy đủ họ tên)

BM/V.ĐMSTCĐS/24

TRƯỜNG ĐẠI HỌC
TÀI CHÍNH - MARKETING
VIỆN ĐỔI MỚI SÁNG TẠO
VÀ CHUYỂN ĐỔI SỐ

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

Thành phố Hồ Chí Minh, ngày ... tháng ... năm .....

THÔNG BÁO SỰ CỐ BẤT THƯỜNG TRUY CẬP HỆ THỐNG MÁY CHỦ

Kính gửi: .....

Đơn vị phụ trách: .....

Thời gian phát hiện sự cố: ..... giờ ..... phút, ngày ..... tháng ..... năm .....

Địa điểm: .....

Người phát hiện sự cố:

- Họ và tên: .....
- Chức vụ: .....
- Đơn vị công tác: .....

1. Mô tả sự cố:

- Loại sự cố: □ Truy cập trái phép □ Tấn công mạng □ Rò rỉ dữ liệu □ Khác: .....
- Hệ thống bị ảnh hưởng: .....
- Tài khoản liên quan (nếu có): .....
- IP truy cập bất thường: .....
- Thời điểm truy cập: .....

2. Biện pháp xử lý ban đầu:

- Ngắt kết nối thiết bị khỏi hệ thống: □ Có □ Không
- Thông báo cho bộ phận an ninh mạng: □ Đã thông báo □ Chưa thông báo
- Ghi nhận log hệ thống: □ Có □ Không
- Các biện pháp khác: .....

3. Đề xuất và kiến nghị

.....

VIỆN ĐMSTCĐS	**NGƯỜI BÁO CÁO**
(Ký, ghi đầy đủ họ tên)	*(Ký, ghi đầy đủ họ tên)*

Nơi nhận:
- Lãnh đạo Viện ĐMSTCĐS;
- Lưu: ĐMSTCĐS.

BM/V.ĐMSTCĐS/24

TRƯỜNG ĐẠI HỌC
TÀI CHÍNH - MARKETING
VIỆN ĐỔI MỚI SÁNG TẠO
VÀ CHUYỂN ĐỔI SỐ

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

Thành phố Hồ Chí Minh, ngày ... tháng ... năm ... ...

BÁO CÁO HOÀN THÀNH CÔNG VIỆC

1.Thông tin thiết bị và người sử dụng:

- Họ và tên: .....
- Đơn vị công tác: .....
- Loại thiết bị: .....
- Nhãn hiệu – Model: .....
- Hệ điều hành: .....
- Tài khoản truy cập hệ thống: .....

2. Nội dung công việc đã thực hiện:

- Mô tả chi tiết các công việc đã thực hiện liên quan đến truy cập hệ thống máy chủ bằng thiết bị cá nhân:

.....

.....

.....

.....

.....

3. Đánh giá kết quả và tuân thủ:

- Thiết bị đảm bảo tuân thủ các quy định về an toàn thông tin: □ Có □ Không
- Không phát hiện sự cố bất thường trong quá trình truy cập: □ Đúng □ Sai
- Các biện pháp bảo mật đã áp dụng: .....

4. Kiến nghị *(nếu có)*:

.....

.....

NGƯỜI BÁO CÁO
(Ký, ghi đầy đủ họ tên)

BM/V.ĐMSTCĐS/25

TRƯỜNG ĐẠI HỌC
TÀI CHÍNH - MARKETING
ĐỘI ỨNG CỨU ATTT MẠNG

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

Thành phố Hồ Chí Minh, ngày ... tháng ... năm .....

BIÊN BẢN
BÁO CÁO SỰ CỐ AN TOÀN THÔNG TIN MẠNG

1. Họ và tên người phát hiện: .....

2. Đơn vị công tác: .....

3. Tên sự cố: .....

.....

4. Các dấu hiệu nhận biết *(bằng chữ)*:

.....

.....

.....

.....

5. Các minh chứng *(bằng hình ảnh nếu có)*:

.....

.....

.....

.....

6. Thời điểm phát hiện: .....

(Ví dụ: Lúc 9g29 ngày 07/7/2025)

7. Địa điểm phát hiện: .....

(Ví dụ: Phòng A.205 Trụ sở 778 Nguyễn Kiệm)

ĐỘI ỨNG CỨU ATTT MẠNG **NGƯỜI PHÁT HIỆN**

Mã tiếp nhận:

Nơi nhận:
- Lãnh đạo Viện ĐMSTCĐS;
- Lưu: ĐMSTCĐS.

BM/V.ĐMSTCĐS/25

TRƯỜNG ĐẠI HỌC
TÀI CHÍNH - MARKETING
VIỆN ĐỔI MỚI SÁNG TẠO
VÀ CHUYỂN ĐỔI SỐ

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

Thành phố Hồ Chí Minh, ngày ... tháng ... năm ... ...

BIÊN BẢN TIẾP NHẬN SỰ CỐ
ĐÁNH GIÁ PHÂN LOẠI SỰ CỐ AN TOÀN THÔNG TIN MẠNG

1. Mã tiếp nhận: .....

2. Loại sự cố:

□ Sự cố hạ tầng mạng

□ Sự cố máy chủ

□ Sự cố phần mềm

□ Sự cố rò rỉ thông tin

□ Khác

Ghi rõ: .....

3. Mức độ sự cố *(1, 2 hoặc 3)*:.....

- Mức độ 1 (Thấp): sự cố không ảnh hưởng đến hoạt động chung của Trường.

- Mức độ 2 (Trung bình): sự cố ảnh hưởng một phần hệ thống nhưng chưa gây gián đoạn lớn.

- Mức độ 3 (Cao): gây gián đoạn nghiêm trọng, rò rỉ dữ liệu hoặc ảnh hưởng diện rộng tới hoạt động chung của Trường.

4. Hệ thống thông tin bị ảnh hưởng *(liệt kê tất cả)*:

.....

.....

5. Đánh giá chung *(nếu có)*:

.....

.....

6. Lưu ý *(quan trọng nếu có)*:.....

ĐỘI ỨNG CỨU ATTT MẠNG **VIỆN ĐMSTCĐS**

Nơi nhận:
- Lãnh đạo Viện ĐMSTCĐS;
- Lưu: ĐMSTCĐS.

BM/V.ĐMSTCĐS/25

TRƯỜNG ĐẠI HỌC
TÀI CHÍNH - MARKETING
VIỆN ĐỔI MỚI SÁNG TẠO
VÀ CHUYỂN ĐỔI SỐ

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

Thành phố Hồ Chí Minh, ngày ... tháng ... năm .....

BIÊN BẢN BÁO CÁO
THỰC HIỆN ỨNG CỨU SỰ CỐ AN TOÀN THÔNG TIN MẠNG

1. Mã tiếp nhận: .....

2. Người thực hiện:

STT	Họ và tên	Đơn vị	Công việc
1			
2			
...			

3. Khoảng thời gian thực hiện: .....

4. Báo cáo chi tiết:

.....

.....

.....

.....

.....

5. Lưu ý *(quan trọng nếu có)*:.....

ĐỘI ỨNG CỨU ATTT MẠNG **VIỆN ĐMSTCĐS**

Nơi nhận:
- Lãnh đạo Viện ĐMSTCĐS;
- Lưu: ĐMSTCĐS.

BM/V.ĐMSTCĐS/25

TRƯỜNG ĐẠI HỌC
TÀI CHÍNH - MARKETING
VIỆN ĐỔI MỚI SÁNG TẠO
VÀ CHUYỂN ĐỔI SỐ

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

Thành phố Hồ Chí Minh, ngày ... tháng ... năm .....

BIÊN BẢN BÁO CÁO ĐÁNH GIÁ HỆ THỐNG SAU THỰC HIỆN ỨNG CỨU SỰ CỐ AN TOÀN THÔNG TIN MẠNG

1. Mã tiếp nhận: .....

2. Người thực hiện:

STT	Họ và tên	Đơn vị	Công việc
1			
2			

3. Báo cáo chi tiết *(tất cả hệ thống thông tin liên quan)*:

- Hệ thống thông tin 1:.....

+ Trước ứng cứu:.....

+ Sau ứng cứu:.....

.....

+ Đánh giá: .....

- Hệ thống thông tin 2:.....

+ Trước ứng cứu:.....

.....

+ Sau ứng cứu:.....

.....

+ Đánh giá: .....

.....

4. Lưu ý *(quan trọng nếu có)*:.....

ĐỘI ỨNG CỨU ATTT MẠNG **VIỆN ĐMSTCĐS**

Nơi nhận:
- Lãnh đạo Viện ĐMSTCĐS;
- Lưu: ĐMSTCĐS.

BM/V.ĐMSTCĐS/25

TRƯỜNG ĐẠI HỌC
TÀI CHÍNH - MARKETING
VIỆN ĐỔI MỚI SÁNG TẠO
VÀ CHUYỂN ĐỔI SỐ

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

Thành phố Hồ Chí Minh, ngày ... tháng ... năm .....

BIÊN BẢN TỔNG HỢP
SAU THỰC HIỆN ỨNG CỨU SỰ CỐ AN TOÀN THÔNG TIN MẠNG

1. Mã tiếp nhận:.....

2. Báo cáo rút kinh nghiệm:

.....

.....

.....

.....

.....

.....

.....

.....

3. Kiến nghị *(nếu có)*:

.....

.....

.....

.....

.....

ĐỘI ỨNG CỨU ATTT MẠNG **VIỆN ĐMSTCĐS**

Nơi nhận:
- Lãnh đạo Viện ĐMSTCĐS;
- Lưu: ĐMSTCĐS.

BIỂU MẪU KIỂM TRA, TỰ ĐÁNH GIÁ ĐỊNH KỲ VỀ AN TOÀN, AN NINH MẠNG

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

I. Thông tin chung:

Tên đơn vị kiểm tra	.....
Thời gian thực hiện kiểm tra	Từ ..... đến .....
Người phụ trách kiểm tra	.....
Chức vụ / Thành phần tham gia	.....

II. Nội dung tự kiểm tra:

STT	Nội dung kiểm tra	Kết quả (✓/✗)	Mức độ tuân thủ (Điểm từ 1–5)	Ghi chú/ Minh chứng
1	Quản lý và sử dụng tài khoản truy cập đúng quy định (đổi mật khẩu, không chia sẻ tài khoản, sử dụng MFA nếu có)			
2	Thực hiện sao lưu dữ liệu định kỳ; dữ liệu được bảo mật và phân quyền truy cập hợp lý			
3	Tuân thủ quy định về cài đặt phần mềm (chỉ dùng phần mềm được cấp phép, không cài phần mềm không rõ nguồn gốc)			
4	Thiết bị CNTT (máy tính, điện thoại, USB...) có phần mềm chống mã độc, được cập nhật thường xuyên			
5	Nhật ký bảo mật (log) và thực hiện vá lỗi hệ thống			
6	Kết nối mạng nội bộ của Trường thông qua kênh an toàn (VPN hoặc mạng Wi-Fi nội bộ được bảo mật)			
7	Bảo vệ thông tin cá nhân và tài liệu nội bộ trong hoạt động giảng dạy, học tập, nghiên cứu			
8	Báo cáo kịp thời khi có sự cố hoặc rủi ro an toàn thông tin (ví dụ: nghi ngờ lộ mật khẩu, virus, email giả mạo,...)			
9	Đơn vị đã cử cán bộ, viên chức tham gia tập huấn, tuyên truyền, diễn tập an toàn thông tin theo kế hoạch của Trường			
10	Đơn vị có tuyên truyền, phổ biến nội quy an toàn thông tin đến viên chức, người lao động và người học (tùy theo chức năng của từng đơn vị)			
11	Các đề xuất, kiến nghị nhằm nâng cao công tác bảo đảm an toàn, an ninh mạng			

Mức độ đạt yêu cầu: ☐ Đạt ☐ Chưa đạt ☐ Cần cải thiện

III. Tổng hợp đánh giá:

Tổng số nội dung đạt yêu cầu: ...../10

Nội dung chưa đạt (nếu có): .....

Biện pháp khắc phục, thời hạn hoàn thành: .....

IV. Xác nhận

Người lập biểu	Viện ĐMST&CĐS	Người đứng đầu đơn vị
Ký, ghi rõ họ tên, ngày lập	Ký, ghi rõ họ tên, ngày kiểm tra	Ký tên, đóng dấu (nếu có)

Ghi chú:

- Biểu mẫu này được sử dụng định kỳ 02 lần/năm (mỗi 06 tháng/lần).

- Kết quả gửi về Viện Đổi mới sáng tạo và Chuyển đổi số chậm nhất 10 ngày sau khi hoàn tất tự kiểm tra.

- Các minh chứng (ảnh chụp, biên bản, báo cáo kỹ thuật, danh sách tập huấn,...) được lưu kèm hồ sơ kiểm tra của đơn vị.