BỘ TÀI CHÍNH
TRƯỜNG ĐẠI HỌC
TÀI CHÍNH – MARKETING

Số: 3998/QĐ-ĐHTCM

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

Thành phố Hồ Chí Minh, ngày 02 tháng 12 năm 2025

QUYẾT ĐỊNH
Ban hành Quy chế Bảo vệ dữ liệu cá nhân 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 Luật Bảo vệ quyền lợi người tiêu dùng số 19/2023/QH15 ngày 20/6/2023 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 15/7/2013 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 trưởng 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 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 2813/QĐ-BTC ngày 20/12/2023 của Bộ trưởng Bộ Tài chính ban hành Quy chế Bảo vệ dữ liệu cá nhân tại Bộ Tài chính;

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 3887/QĐ-ĐHCM ngày 25/11/2025 của Hiệu trưởng Trường Đại học Tài chính - Marketing ban hành Quy định về chức năng, nhiệm vụ và quyền hạn của các đơn vị thuộc và trực thuộc Trường Đại học Tài chính - Marketing;

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;

Căn cứ Quyết định số 8684/QĐ-ĐHTCM ngày 10/11/2025 của Hiệu trưởng Trường Đại học Tài chính - Marketing ban hành Quy chế An toàn thông tin và An ninh mạng của Trường Đại học Tài chính - Marketing;

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 Bảo vệ dữ liệu cá nhân của Trường Đại học Tài chính - Marketing".

Điều 2. Quyết định có hiệu lực thi hành kể từ ngày ký. Trưởng các đơn vị, 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;
- Website UFM;
- Lưu: VT, ĐMSTCĐS (03b).

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
Bảo vệ dữ liệu cá nhân của Trường Đại học Tài chính – Marketing

(Ban hành kèm theo Quyết định số 3998/QĐ-ĐHTCM ngày 02 tháng 12 năm 2025 của Hiệu trưởng Trường Đại học Tài chính – Marketing)

Chương I
QUY ĐỊNH CHUNG

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

1. Quy chế này quy định về việc thu thập, lưu trữ, sử dụng, chia sẻ và xử lý dữ liệu cá nhân trong phạm vi hoạt động của Trường Đại học Tài chính – Marketing (sau đây gọi tắt là Trường).

2. Quy chế này áp dụng đối với:

a) Viên chức, người lao động, cộng tác viên đang làm việc tại Trường.

b) Người học (sinh viên, học viên, nghiên cứu sinh) đang học tập tại Trường.

c) Các cơ quan, tổ chức, cá nhân bên thứ ba có hợp đồng, thỏa thuận hoặc hợp tác xử lý dữ liệu cá nhân với Trường.

Điều 2. Giải thích từ ngữ

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

1. *Dữ liệu cá nhân*: là thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc các dạng tương tự, gắn liền với một cá nhân cụ thể hoặc có thể giúp nhận dạng cá nhân đó.

2. *Dữ liệu cá nhân cơ bản*: là các thông tin cơ bản gắn với cá nhân, bao gồm họ tên, ngày sinh, số định danh, thông tin liên hệ, học tập, công tác.

3. *Dữ liệu cá nhân nhạy cảm*: là các thông tin liên quan đến đời sống riêng tư hoặc các lĩnh vực đặc biệt của cá nhân, bao gồm sức khỏe, tài chính, dữ liệu sinh trắc học, lịch sử kỷ luật, quan điểm cá nhân.

4. *Dữ liệu cá nhân đã được ẩn danh*: là dữ liệu cá nhân được xử lý theo cách để không thể gắn trực tiếp với một cá nhân cụ thể, trừ khi có thêm thông tin bổ sung.

5. *Dữ liệu giả danh hóa hoàn toàn*: là dữ liệu cá nhân đã được xử lý bằng biện pháp kỹ thuật, nghiệp vụ để loại bỏ vĩnh viễn mọi yếu tố định danh. Dữ liệu này không còn khả năng nhận dạng, truy vết hoặc liên kết với cá nhân cụ thể nào, ngay cả khi kết hợp với các nguồn dữ liệu khác.

6. *Chủ thể dữ liệu cá nhân*: là cá nhân có dữ liệu cá nhân được thu thập, lưu trữ, xử lý trong phạm vi hoạt động của Trường Đại học Tài chính – Marketing.

7. *Xử lý dữ liệu cá nhân*: là hoạt động một phần hoặc toàn bộ theo quy trình, bao gồm thu thập, ghi, lưu trữ, chỉnh sửa, sao chép, truy cập, truy xuất, sử dụng, phân tích, xác minh, cung cấp, chia sẻ, chuyển giao, công bố, xóa, tiêu hủy dữ liệu cá nhân bằng phương pháp thủ công hoặc tự động. Việc xử lý dữ liệu cá nhân tại Trường Đại học Tài chính – Marketing phải được thực hiện đúng mục đích, trong phạm vi được phép và có sự đồng ý của chủ thể dữ liệu, trừ trường hợp pháp luật có quy định khác.

8. *Bên kiểm soát dữ liệu cá nhân*: là tổ chức, cá nhân quyết định mục đích và phương thức xử lý dữ liệu cá nhân.

9. *Bên xử lý dữ liệu cá nhân*: là tổ chức, cá nhân thực hiện việc xử lý dữ liệu cá nhân thay mặt cho bên kiểm soát.

10. *Bên kiểm soát và xử lý dữ liệu cá nhân*: là tổ chức, cá nhân vừa quyết định, vừa trực tiếp thực hiện hoạt động xử lý.

11. *Hệ thống thông tin xử lý dữ liệu cá nhân*: là hệ thống có chức năng thu thập, lưu trữ, quản lý, khai thác và chia sẻ dữ liệu cá nhân.

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

13. *Đơn vị vận hành hệ thống thông tin*: là đơn vị được giao nhiệm vụ quản lý, vận hành và đảm bảo hoạt động kỹ thuật ổn định của các hệ thống thông tin.

14. *Đánh giá tác động xử lý dữ liệu cá nhân*: là hoạt động xem xét, xác định và phân tích các rủi ro có thể phát sinh đối với quyền và lợi ích hợp pháp của chủ thể dữ liệu; đồng thời ghi nhận các biện pháp quản lý, kiểm soát rủi ro khi Nhà trường tiến hành xử lý dữ liệu cá nhân.

15. *Ứng cứu sự cố an toàn thông tin*: là hoạt động phát hiện, phân tích, xử lý, khắc phục và phục hồi hệ thống, dữ liệu và dịch vụ sau khi xảy ra sự cố an toàn thông tin nhằm giảm thiểu thiệt hại và khôi phục hoạt động bình thường.

16. *Sự cố, rủi ro an toàn dữ liệu*: là sự kiện hoặc tình huống bất thường gây ra hoặc có khả năng gây ra mất dữ liệu, thay đổi dữ liệu, rò rỉ dữ liệu, truy cập trái phép hoặc gián đoạn dữ liệu cá nhân trong quá trình xử lý.

17. *Vi phạm dữ liệu cá nhân*: là hành vi dẫn đến rò rỉ, mất mát, truy cập trái phép, sử dụng trái phép, thay đổi trái phép, tiết lộ trái phép hoặc tiêu hủy trái phép dữ liệu cá nhân, gây ảnh hưởng đến quyền và lợi ích hợp pháp của chủ thể dữ liệu.

Điều 3. Phạm vi bảo vệ dữ liệu cá nhân

1. Quy chế này quy định việc thu thập, lưu trữ, xử lý, sử dụng, chia sẻ, truyền tải, bảo mật và tiêu hủy dữ liệu cá nhân của viên chức, người lao động, người học, đối tác, khách hàng và các bên có liên quan trong toàn Trường Đại học Tài chính – Marketing.

2. Dữ liệu cá nhân được bảo vệ trong suốt vòng đời xử lý, bao gồm các giai đoạn: thu thập, lưu trữ, khai thác, chia sẻ và tiêu hủy, bảo đảm nguyên tắc toàn vẹn, bảo mật và khả dụng của dữ liệu.

3. Việc bảo vệ dữ liệu cá nhân được áp dụng đối với mọi hoạt động xử lý dữ liệu do Trường thực hiện hoặc ủy quyền cho tổ chức, cá nhân khác thực hiện trong phạm vi nhiệm vụ, quyền hạn được giao.

4. Các hệ thống, thiết bị, nền tảng xử lý dữ liệu cá nhân thuộc quyền quản lý, khai thác, vận hành hoặc thuê ngoài của Trường.

5. Các đơn vị, cá nhân và đối tác bên ngoài khi tham gia quản lý, khai thác, cung cấp dịch vụ liên quan đến dữ liệu cá nhân của Trường phải tuân thủ đầy đủ các quy định trong Quy chế này. Mọi hành vi vi phạm đều bị xem xét, xử lý theo quy định của pháp luật hiện hành.

Điều 4. Nguyên tắc bảo vệ dữ liệu cá nhân

1. Việc bảo vệ dữ liệu cá nhân tại Trường phải được thực hiện một cách nghiêm túc và đầy đủ, tuân thủ pháp luật hiện hành và các quy chế, quy định nội bộ của Trường.

2. Nguyên tắc minh bạch: mọi hoạt động xử lý dữ liệu cá nhân phải được thông báo rõ ràng, công khai cho chủ thể dữ liệu về mục đích, phạm vi, phương thức và thời gian xử lý.

3. Nguyên tắc giới hạn mục đích: dữ liệu cá nhân chỉ được thu thập, sử dụng cho các mục đích cụ thể, hợp pháp và đã được chủ thể dữ liệu đồng ý; không được xử lý ngoài phạm vi đó.

4. Nguyên tắc giảm thiểu dữ liệu: chỉ thu thập và lưu trữ những dữ liệu thực sự cần thiết cho mục đích xử lý; hạn chế tối đa việc xử lý dữ liệu không liên quan hoặc vượt quá yêu cầu.

5. Nguyên tắc chính xác và cập nhật: dữ liệu cá nhân phải được bảo đảm chính xác, đầy đủ và được cập nhật kịp thời khi có thay đổi.

6. Nguyên tắc bảo mật và an toàn: áp dụng các biện pháp kỹ thuật và tổ chức phù hợp để bảo đảm an toàn, ngăn chặn truy cập, rò rỉ, mất mát hoặc hủy hoại dữ liệu trái phép.

Điều 5. Phân loại dữ liệu

1. Nhóm dữ liệu cá nhân cơ bản: là các thông tin nhận dạng ban đầu của chủ thể dữ liệu, được sử dụng để xác định danh tính và phục vụ công tác hành chính, đào tạo, nghiên cứu, quản lý nhân sự, bao gồm:

a) Họ, tên, ngày tháng năm sinh, giới tính, quốc tịch.

b) Số định danh cá nhân, số CCCD/Hộ chiếu, mã số sinh viên/học viên, mã viên chức/người lao động.

c) Thông tin liên hệ: địa chỉ thường trú, địa chỉ tạm trú, địa chỉ liên hệ, email, số điện thoại, mã bưu chính.

d) Thông tin học tập và hành chính cơ bản: lớp, khoa, đơn vị công tác, kết quả học tập, bậc lương, hợp đồng, tài khoản ngân hàng trả lương/học phí.

2. Nhóm dữ liệu cá nhân phát sinh điện tử, hồ sơ kỹ thuật số: là các thông tin được hình thành, lưu trữ hoặc xử lý trên môi trường điện tử trong quá trình học tập, giảng dạy, làm việc, giao dịch hành chính, bao gồm:

a) Thông tin đăng nhập, định danh kỹ thuật số và lịch sử truy cập vào hạ tầng công nghệ thông tin, hệ thống thông tin, cổng dịch vụ công, hệ thống đào tạo, thi trực tuyến, email, hoặc các ứng dụng nội bộ của Trường.

b) Dữ liệu hoạt động học tập, khảo thí, nghiên cứu, tương tác qua các nền tảng và hệ thống quản lý học tập (LMS, e-Learning, Google Workspace, Microsoft 365,...).

c) Hồ sơ xử lý nghiệp vụ số: biểu mẫu điện tử, quyết định, văn bản số hóa, hồ sơ học tập hoặc nhân sự lưu trữ trực tuyến.

d) Dữ liệu thu thập từ hệ thống giám sát hình ảnh, cổng dịch vụ công trực tuyến, nền tảng học tập, hệ thống tuyển sinh, và hệ thống khảo thí trực tuyến của Trường.

e) Thông tin giao dịch điện tử và nhật ký hệ thống liên quan đến bảo mật, sao lưu, khôi phục, chứng thực điện tử.

3. Nhóm dữ liệu cá nhân nhạy cảm

Là dữ liệu có tính riêng tư cao, nếu bị tiết lộ có thể gây ảnh hưởng đến quyền, lợi ích hợp pháp, danh dự, nhân phẩm của chủ thể dữ liệu. Bao gồm:

a) Thông tin về tình trạng sức khỏe, hồ sơ y tế, tiền sử bệnh, dữ liệu sinh trắc học (vân tay, khuôn mặt, giọng nói,...).

b) Dữ liệu tài chính cá nhân: thu nhập, tài sản, tài khoản, giao dịch, thuế, bảo hiểm, học bổng, hỗ trợ xã hội.

c) Thông tin về quan điểm chính trị, tôn giáo, nghề nghiệp, quan hệ xã hội hoặc thông tin kỷ luật, đánh giá cá nhân.

d) Dữ liệu định vị, hình ảnh, âm thanh, video được thu thập qua hệ thống giám sát hình ảnh, thiết bị điện tử, nền tảng học trực tuyến, hoặc phương tiện của Trường.

4. Nguyên tắc quản lý và cập nhật dữ liệu

a) Mỗi nhóm dữ liệu được áp dụng biện pháp bảo mật tương ứng theo nhóm và mức độ nhạy cảm.

b) Việc mở rộng, thu hẹp hoặc thay đổi phạm vi dữ liệu cá nhân phải được thực hiện trên cơ sở đánh giá tác động và tuân thủ quy định của pháp luật.

c) Mọi thay đổi phạm vi dữ liệu phải được Viện Đổi mới sáng tạo và Chuyển đổi số xem xét, thẩm định và trình Ban Giám hiệu phê duyệt trước khi áp dụng.

Điều 6. Phân công vai trò kiểm soát và xử lý dữ liệu cá nhân

1. Viện Đổi mới sáng tạo và Chuyển đổi số là đơn vị đầu mối kiểm soát và xử lý dữ liệu cá nhân trong toàn Trường, chịu trách nhiệm tham mưu, giám sát, kiểm tra, hướng dẫn các đơn vị triển khai.

2. Các đơn vị thuộc Trường có trách nhiệm xử lý dữ liệu cá nhân theo phạm vi chức năng được giao và chịu trách nhiệm về an toàn thông tin của hệ thống quản lý dữ liệu do mình vận hành.

3. Khi có thay đổi trong quy trình xử lý dữ liệu, các đơn vị phải thông báo và cần có ý kiến của Viện Đổi mới sáng tạo và Chuyển đổi số trước khi triển khai.

4. Trường hợp Trường thuê ngoài dịch vụ công nghệ thông tin, hạ tầng công nghệ đám mây hoặc lưu trữ dữ liệu, đơn vị cung cấp dịch vụ phải ký cam kết bảo mật và chịu trách nhiệm như bên xử lý dữ liệu cá nhân.

5. Viện Đổi mới sáng tạo và Chuyển đổi số có quyền yêu cầu đơn vị cung cấp thông tin, hồ sơ kỹ thuật để kiểm tra việc tuân thủ trong xử lý dữ liệu cá nhân.

Điều 7. Các hành vi bị nghiêm cấm

1. Hành vi vi phạm trong thu thập, xử lý dữ liệu cá nhân

a) Thu thập, xử lý, sử dụng, chia sẻ dữ liệu cá nhân của người học, viên chức, người lao động khi chưa có sự đồng ý của chủ thể dữ liệu hoặc không đúng mục đích, phạm vi được phê duyệt.

b) Cung cấp, chuyển giao, tiết lộ hoặc mua bán dữ liệu cá nhân cho bên thứ ba trái với quy định của pháp luật hoặc của Trường.

c) Lợi dụng việc xử lý dữ liệu cá nhân để thu lợi bất chính, gây ảnh hưởng đến quyền, lợi ích hợp pháp của chủ thể dữ liệu hoặc của Trường.

2. Hành vi vi phạm trong quản lý, bảo mật dữ liệu cá nhân

a) Không thực hiện, hoặc thực hiện không đầy đủ các biện pháp bảo vệ dữ liệu cá nhân theo quy định của Quy chế này.

b) Cấp quyền truy cập, chỉnh sửa, chia sẻ dữ liệu cá nhân cho cá nhân hoặc tổ chức khác khi chưa được phê duyệt hoặc không đúng thẩm quyền.

c) Không thực hiện đầy đủ nghĩa vụ bảo mật dữ liệu cá nhân, bao gồm: không báo cáo, chậm báo cáo hoặc cố tình che giấu sự cố, rò rỉ, mất dữ liệu cá nhân khi phát hiện.

d) Tự ý lưu trữ, sao chép, chụp ảnh, trích xuất hoặc chuyển dữ liệu cá nhân ra thiết bị cá nhân, tài khoản riêng hoặc nền tảng bên ngoài hệ thống của Trường khi chưa được phê duyệt.

e) Khai thác, sử dụng hoặc lưu trữ dữ liệu cá nhân cho mục đích cá nhân, thương mại hoặc ngoài nhiệm vụ được giao.

f) Không tuân thủ quy trình ứng cứu sự cố, khắc phục rò rỉ dữ liệu cá nhân theo hướng dẫn của Viện Đổi mới sáng tạo và Chuyển đổi số.

3. Hành vi vi phạm về sử dụng hệ thống thông tin và hạ tầng kỹ thuật

a) Truy cập, thay đổi, phá hoại, xóa bỏ hoặc làm gián đoạn hoạt động của hệ thống thông tin, thiết bị lưu trữ dữ liệu cá nhân của Trường.

b) Cài đặt, sử dụng phần mềm trái phép hoặc công cụ có nguy cơ gây mất an toàn dữ liệu.

c) Kết nối thiết bị lưu trữ, truyền dữ liệu cá nhân với mạng công cộng, dịch vụ lưu trữ đám mây chưa được kiểm soát hoặc phê duyệt.

4. Hành vi vi phạm khác

a) Giả mạo, xuyên tạc, tiết lộ thông tin cá nhân của người học, viên chức, người lao động gây ảnh hưởng đến danh dự, nhân phẩm, uy tín hoặc quyền, lợi ích hợp pháp của họ.

b) Từ chối, cản trở việc thực hiện quyền của chủ thể dữ liệu (quyền được biết, truy cập, chỉnh sửa, xóa, hạn chế hoặc phản đối xử lý dữ liệu).

c) Không tuân thủ quy trình, hướng dẫn, quy định về bảo mật thông tin do Trường ban hành.

d) Các hành vi khác vi phạm quy định của pháp luật về bảo vệ dữ liệu cá nhân, an toàn thông tin mạng, an ninh mạng và các quy định nội bộ của Trường.

Chương II

TRÁCH NHIỆM VÀ NGHĨA VỤ

Điều 8. Trách nhiệm của Trường

1. Ban hành các quy trình, hướng dẫn kỹ thuật về bảo mật dữ liệu cá nhân.

2. Đầu tư hạ tầng công nghệ thông tin: mã hóa, tường lửa, sao lưu dữ liệu, giám sát truy cập.

3. Tổ chức đào tạo, tập huấn định kỳ về an toàn dữ liệu và an ninh mạng cho viên chức, người lao động và người học toàn Trường.

4. Tổ chức kiểm tra, giám sát định kỳ và đột xuất việc thực hiện công tác bảo vệ dữ liệu cá nhân tại các đơn vị; tổng hợp, đánh giá và báo cáo kết quả cho Bộ chủ quản hoặc cơ quan có thẩm quyền khi được yêu cầu.

5. Bố trí kinh phí hằng năm trong kế hoạch tài chính để đầu tư, nâng cấp hạ tầng bảo mật, duy trì an toàn, an ninh mạng.

Điều 9. Trách nhiệm của các đơn vị thuộc và trực thuộc Trường

1. Mỗi đơn vị thuộc và trực thuộc Trường phải phân công nhân sự phụ trách bảo mật dữ liệu của đơn vị mình quản lý.

2. Các đơn vị đảm bảo việc phân quyền truy cập và chỉ sử dụng dữ liệu đúng chức năng, nhiệm vụ được giao.

3. Tổ chức phổ biến, tuyên truyền và đào tạo nội bộ về bảo vệ dữ liệu cá nhân cho viên chức, người lao động và người học thuộc phạm vi quản lý.

4. Ngay sau khi phát hiện sự cố hoặc rủi ro, đơn vị phải ghi nhận đầy đủ thông tin liên quan (thời gian xảy ra, loại sự cố, phạm vi ảnh hưởng, biện pháp tạm thời đã thực hiện) và báo cáo kịp thời cho Viện Đổi mới sáng tạo và Chuyển đổi số để phối hợp xử lý.

5. Định kỳ 06 tháng/lần báo cáo tình hình bảo vệ dữ liệu cá nhân và an toàn thông tin cho Viện Đổi mới sáng tạo và Chuyển đổi số.

6. Người đứng đầu đơn vị chịu trách nhiệm trước Hiệu trưởng và bị xử lý theo quy định nếu để xảy ra rò rỉ dữ liệu cá nhân trong phạm vi quản lý của đơn vị mình.

Điều 10. Trách nhiệm của cá nhân

1. Nguyên tắc chung

a) Mỗi cá nhân trong phạm vi thuộc Trường có trách nhiệm chủ động bảo vệ dữ liệu cá nhân của bản thân và của người khác trong quá trình học tập, công tác, nghiên cứu, hoặc thực hiện nhiệm vụ được giao.

b) Mọi hành vi xử lý, truy cập, sử dụng hoặc chia sẻ dữ liệu cá nhân phải tuân thủ đúng mục đích, giới hạn phạm vi cho phép và được phê duyệt theo quy định của Trường.

2. Nghĩa vụ của cá nhân

a) Thực hiện nghiêm các quy định của pháp luật, Quy chế này và các hướng dẫn liên quan đến bảo vệ dữ liệu cá nhân, an toàn, an ninh mạng, và bảo mật thông tin trong Trường.

b) Bảo đảm an toàn cho tài khoản truy cập, mật khẩu, thiết bị cá nhân khi sử dụng hệ thống công nghệ thông tin, phần mềm hoặc nền tảng số của Trường.

c) Cá nhân phải bảo đảm cập nhật thông tin liên hệ chính thức (hộp thư điện tử, tài khoản truy cập đã được Trường cấp) khi sử dụng các nền tảng, hệ thống do Trường quản lý, nhằm bảo đảm thông tin xác thực và thông báo kịp thời khi có sự cố liên quan đến dữ liệu cá nhân.

d) Không chia sẻ thông tin đăng nhập, mật khẩu, mã xác thực cho người khác dưới bất kỳ hình thức nào.

e) Khi phát hiện sự cố, rủi ro, hoặc nghi ngờ rò rỉ dữ liệu cá nhân, cá nhân phải báo cáo ngay cho đơn vị trực thuộc hoặc Viện Đổi mới sáng tạo và Chuyển đổi số để được hướng dẫn xử lý. Không tự ý khắc phục, xóa hoặc sao chép dữ liệu liên quan đến sự cố khi chưa được phép.

f) Chỉ được thu thập, truy cập, hoặc sử dụng dữ liệu cá nhân trong phạm vi công việc, nhiệm vụ được giao và phải được sự đồng ý của chủ thể dữ liệu hoặc cơ quan có thẩm quyền.

g) Không chia sẻ, phát tán, sao chép, hoặc đăng tải dữ liệu cá nhân của người khác lên các nền tảng mạng xã hội, dịch vụ lưu trữ đám mây, hay phương tiện truyền thông khi chưa có sự phê duyệt của Trường.

h) Tham dự đầy đủ các chương trình tập huấn, tuyên truyền, hoặc kiểm tra về an toàn thông tin, bảo vệ dữ liệu cá nhân do Trường hoặc Viện Đổi mới sáng tạo và Chuyển đổi số tổ chức.

i) Tiếp tục giữ bí mật, không tiết lộ, không sử dụng, không chuyển giao dữ liệu hoặc tài liệu cá nhân mà mình có được trong thời gian làm việc, học tập, kể cả sau khi nghỉ việc, chuyển công tác hoặc tốt nghiệp.

3. Quyền của cá nhân là chủ thể dữ liệu

a) Quyền được biết: cá nhân được thông báo về mục đích, phạm vi, phương thức và thời gian xử lý dữ liệu cá nhân của mình.

b) Quyền truy cập và chỉnh sửa: cá nhân được truy cập, kiểm tra, yêu cầu sửa đổi dữ liệu cá nhân nếu phát hiện sai lệch hoặc không còn phù hợp.

c) Quyền hạn chế hoặc xóa dữ liệu: cá nhân được yêu cầu hạn chế xử lý hoặc xóa dữ liệu cá nhân của mình trong phạm vi pháp luật cho phép.

d) Quyền phản ánh và khiếu nại: cá nhân có quyền gửi phản ánh, khiếu nại và được thông báo bằng văn bản về kết quả xử lý.

e) Cá nhân có quyền yêu cầu Trường cung cấp thông tin về bên thứ ba được chia sẻ dữ liệu của mình.

4. Trách nhiệm pháp lý: cá nhân vi phạm quy định về bảo vệ dữ liệu cá nhân, tiết lộ hoặc làm rò rỉ thông tin trái phép, gây thiệt hại cho người khác hoặc cho Trường, tùy theo tính chất, mức độ vi phạm sẽ bị xử lý kỷ luật, bồi thường thiệt hại hoặc truy cứu trách nhiệm theo quy định của pháp luật.

Điều 11. Trách nhiệm của Viện Đổi mới sáng tạo và Chuyển đổi số

1. Nhiệm vụ tổ chức, hướng dẫn

a) Là đơn vị đầu mối giúp Hiệu trưởng tổ chức triển khai, kiểm soát và giám sát công tác bảo vệ dữ liệu cá nhân trong toàn Trường.

b) Tham mưu Hiệu trưởng ban hành, sửa đổi, bổ sung, hướng dẫn thực hiện các quy định, quy trình, biểu mẫu, hồ sơ kỹ thuật liên quan đến bảo vệ dữ liệu cá nhân.

c) Hướng dẫn lập, cập nhật hồ sơ đánh giá tác động xử lý dữ liệu cá nhân theo quy định của pháp luật.

d) Chủ trì, phối hợp với các đơn vị rà soát, đánh giá lại hồ sơ tác động xử lý dữ liệu cá nhân ít nhất một lần mỗi năm hoặc khi có thay đổi đáng kể về mục đích, phạm vi, công nghệ hoặc hạ tầng xử lý dữ liệu. Kết quả đánh giá phải được lưu trữ, báo cáo Hiệu trưởng và làm căn cứ điều chỉnh biện pháp bảo mật, kiểm soát rủi ro.

e) Tiếp nhận, tổng hợp và xử lý thông tin về sự cố, rủi ro, hành vi vi phạm quy định về bảo vệ dữ liệu cá nhân; điều phối hoạt động ứng cứu, khắc phục sự cố.

f) Tổ chức hoặc phối hợp tổ chức với các đơn vị thuộc Trường hoặc đơn vị ngoài Trường để đào tạo, tập huấn, tuyên truyền và diễn tập định kỳ về bảo vệ dữ liệu cá nhân, an toàn thông tin và ứng phó sự cố cho viên chức, người lao động và người học.

g) Xây dựng, cập nhật và hướng dẫn sử dụng các biểu mẫu nội bộ: phiếu đồng ý xử lý dữ liệu, sổ ghi nhận sự cố, kế hoạch bảo vệ dữ liệu.

2. Nhiệm vụ về giám sát và kỹ thuật

a) Thực hiện giám sát, kiểm tra và đánh giá định kỳ, đột xuất mức độ an toàn, an ninh mạng của hệ thống thông tin.

b) Triển khai và hướng dẫn các giải pháp kỹ thuật: phân quyền truy cập, mã hóa dữ liệu, sao lưu, tiêu hủy và phục hồi an toàn.

c) Phối hợp với các đơn vị trong việc lập kế hoạch đầu tư, bảo trì, nâng cấp hạ tầng kỹ thuật, đảm bảo kinh phí và năng lực vận hành hệ thống thông tin an toàn.

3. Nhiệm vụ về phối hợp và báo cáo

a) Phối hợp với các đơn vị thuộc và trực thuộc Trường trong công tác quản lý, chia sẻ, bảo mật dữ liệu cá nhân.

b) Định kỳ 06 tháng/lần tổng hợp, đánh giá và báo cáo Hiệu trưởng về tình hình bảo vệ dữ liệu cá nhân, an toàn thông tin và sự cố mạng.

c) Là đầu mối làm việc và báo cáo với Bộ chủ quản và các cơ quan có thẩm quyền về công tác bảo vệ dữ liệu cá nhân, an toàn, an ninh mạng.

d) Cập nhật, phổ biến chính sách pháp luật mới liên quan đến bảo vệ dữ liệu cá nhân; tham mưu Hiệu trưởng rà soát, điều chỉnh, hoàn thiện Quy chế khi có thay đổi quy định của Nhà nước.

e) Bảo đảm lưu trữ, bảo mật và cung cấp kịp thời hồ sơ, dữ liệu, báo cáo phục vụ công tác thanh tra, kiểm tra hoặc đánh giá nội bộ.

f) Chủ động phát hiện, báo cáo kịp thời nguy cơ tiềm ẩn gây mất an toàn, an ninh mạng và phối hợp ứng cứu, xử lý sự cố với các cơ quan có thẩm quyền.

4. Viện Đổi mới sáng tạo và Chuyển đổi số có quyền yêu cầu đơn vị báo cáo bổ sung hoặc kiểm tra thực tế khi có dấu hiệu rủi ro.

Chương III

QUẢN LÝ, LƯU TRỮ, CHIA SẺ VÀ ỨNG CỨU SỰ CỐ

Điều 12. Quản lý và lưu trữ dữ liệu cá nhân

1. Nguyên tắc quản lý và lưu trữ

a) Việc quản lý và lưu trữ dữ liệu cá nhân là trách nhiệm của mọi đơn vị sử dụng hệ thống thông tin thuộc Trường.

b) Việc thu thập, quản lý, lưu trữ, bảo quản và tiêu hủy dữ liệu cá nhân phải đảm bảo tính bí mật, toàn vẹn, sẵn sàng và xác thực; được thực hiện theo quy trình, tiêu chuẩn kỹ thuật phù hợp với cấp độ hệ thống thông tin của Trường.

c) Dữ liệu cá nhân chỉ được lưu trữ trong thời hạn cần thiết để phục vụ cho mục đích xử lý đã xác định hoặc theo quy định của pháp luật chuyên ngành.

d) Mọi hoạt động xử lý, truy cập, sao lưu, di chuyển và tiêu hủy dữ liệu cá nhân đều phải được kiểm soát, phê duyệt và ghi nhận đầy đủ trong hồ sơ lưu trữ.

2. Sao lưu và phục hồi dữ liệu

a) Dữ liệu cá nhân được sao lưu định kỳ tối thiểu 01 lần/tháng.

b) Mọi hoạt động sao lưu và phục hồi phải có biên bản hoặc nhật ký kỹ thuật ghi nhận thời điểm, người thực hiện và kết quả.

3. Nhật ký truy cập và kiểm tra định kỳ

a) Các hệ thống lưu trữ dữ liệu cá nhân phải có chức năng ghi nhật ký truy cập (log), bao gồm: thời điểm, người truy cập, hành động thực hiện và kết quả.

b) Nhật ký truy cập phải được lưu tối thiểu 12 tháng và kiểm tra định kỳ 02 lần/năm để phục vụ giám sát và truy vết sự cố.

c) Mọi hành vi truy cập, chỉnh sửa, sao chép dữ liệu cá nhân ngoài phạm vi được phân quyền đều bị coi là vi phạm quy định bảo mật và xử lý theo quy định tại Quy chế này và các quy định của pháp luật hiện hành.

4. Tiêu hủy và chấm dứt lưu trữ dữ liệu

a) Dữ liệu cá nhân hết thời hạn lưu trữ hoặc không còn mục đích sử dụng phải được tiêu hủy an toàn bằng biện pháp kỹ thuật phù hợp, đảm bảo không thể khôi phục.

b) Việc tiêu hủy dữ liệu phải được lập biên bản, xác nhận bởi đơn vị quản lý dữ liệu và Viện Đổi mới sáng tạo và Chuyển đổi số, lưu hồ sơ tối thiểu 12 tháng.

c) Trường hợp dữ liệu thuộc diện phải lưu trữ dài hạn theo yêu cầu pháp lý hoặc nghĩa vụ báo cáo, Viện có trách nhiệm chuyển sang hình thức lưu trữ bảo mật chuyên dụng, đảm bảo chỉ người có thẩm quyền được phép truy cập.

Điều 13. Chia sẻ dữ liệu cá nhân

1. Việc chia sẻ dữ liệu cá nhân phải tuân thủ các nguyên tắc:

a) Có mục đích rõ ràng, hợp pháp và phù hợp với phạm vi xử lý dữ liệu đã được công bố.

b) Tối thiểu hóa dữ liệu được chia sẻ, chỉ cung cấp những thông tin cần thiết cho mục đích xử lý.

c) Bảo đảm tính bảo mật, toàn vẹn và khả năng truy vết của dữ liệu trong toàn bộ quá trình chia sẻ.

d) Có sự đồng ý của chủ thể dữ liệu, trừ các trường hợp được pháp luật cho phép xử lý mà không cần sự đồng ý.

2. Phạm vi và thẩm quyền chia sẻ

2.1. Chia sẻ nội bộ trong Trường

a) Các đơn vị thuộc và trực thuộc Trường được phép chia sẻ dữ liệu cá nhân trong phạm vi phục vụ công tác chuyên môn, đào tạo, quản lý và nghiên cứu khoa học.

b) Việc chia sẻ phải có được sự đồng ký của người đứng đầu đơn vị, nêu rõ mục đích, phạm vi, đối tượng nhận dữ liệu.

2.2. Chia sẻ dữ liệu ra bên ngoài Trường

a) Chỉ được thực hiện khi có sự chấp thuận bằng văn bản của Hiệu trưởng hoặc người được ủy quyền.

b) Có sự đồng ý bằng văn bản của chủ thể dữ liệu cá nhân, trừ trường hợp pháp luật và Trường có quy định khác.

c) Phải áp dụng biện pháp kỹ thuật bảo mật trong quá trình truyền và lưu dữ liệu (mã hóa, giới hạn truy cập, xóa dữ liệu tạm thời sau sử dụng).

d) Hợp đồng hoặc cam kết bằng văn bản việc bảo mật giữa Trường và bên nhận dữ liệu, quy định rõ phạm vi, mục đích sử dụng, thời hạn lưu trữ, trách nhiệm bảo mật và biện pháp xử lý vi phạm.

3. Hình thức và kênh chia sẻ dữ liệu

a) Việc chia sẻ dữ liệu được thực hiện qua các nền tảng nội bộ hoặc hệ thống kỹ thuật được Trường phê duyệt.

b) Không sử dụng các nền tảng đám mây công cộng hoặc dịch vụ lưu trữ cá nhân (như Gmail, Google Drive, Dropbox, OneDrive cá nhân, mạng xã hội,...) để chia sẻ dữ liệu cá nhân của Trường, trừ khi được Ban Giám hiệu phê duyệt.

c) Khi chia sẻ qua email hoặc phương tiện truyền dữ liệu ra bên ngoài Trường, phải thực hiện mã hóa nội dung hoặc đính kèm tệp tin có mật khẩu; mật khẩu được gửi qua kênh liên lạc khác.

4. Trách nhiệm của bên nhận dữ liệu

a) Sử dụng dữ liệu đúng mục đích, phạm vi và thời hạn được phê duyệt; không sao chép, tiết lộ hoặc chuyển giao dữ liệu cho bên thứ ba khi chưa được Trường chấp thuận.

b) Thực hiện đầy đủ các biện pháp bảo mật kỹ thuật (mã hóa, kiểm soát truy cập, bảo vệ thiết bị lưu trữ).

c) Ngay khi phát hiện mất mát, rò rỉ hoặc vi phạm dữ liệu, phải thông báo ngay cho Viện Đổi mới sáng tạo và Chuyển đổi số để phối hợp xử lý.

5. Hồ sơ và nhật ký chia sẻ dữ liệu

a) Mỗi lần chia sẻ dữ liệu cá nhân phải được ghi nhận trong hồ sơ chia sẻ dữ liệu, bao gồm: mục đích chia sẻ; danh sách hoặc loại dữ liệu được chia sẻ; đối tượng và đơn vị nhận dữ liệu; ngày, giờ, hình thức, người thực hiện; biện pháp bảo mật đã áp dụng; thời hạn sử dụng và kết quả hủy hoặc thu hồi dữ liệu (nếu có).

b) Nhật ký chia sẻ dữ liệu được hệ thống tự động hoặc đơn vị lưu trữ cập nhật, bảo quản tối thiểu 12 tháng kể từ ngày chia sẻ.

c) Viện Đổi mới sáng tạo và Chuyển đổi số có trách nhiệm tổng hợp, lưu trữ, giám sát hồ sơ chia sẻ dữ liệu; định kỳ kiểm tra, đánh giá việc tuân thủ các nguyên tắc bảo vệ dữ liệu cá nhân.

6. Trách nhiệm giám sát và xử lý vi phạm

a) Viện Đổi mới sáng tạo và Chuyển đổi số chịu trách nhiệm giám sát, đánh giá và tổng hợp báo cáo định kỳ 06 tháng/lần về tình hình chia sẻ dữ liệu cá nhân trong toàn Trường.

b) Đơn vị, cá nhân vi phạm quy định về chia sẻ dữ liệu cá nhân sẽ bị xử lý theo mức độ vi phạm; hình thức xử lý được quy định tại Điều 16 của Quy chế này.

c) Trường hợp vi phạm nghiêm trọng (rò rỉ quy mô lớn, chia sẻ cho bên thứ ba trái phép) phải báo cáo Hiệu trưởng và cơ quan chức năng có thẩm quyền trong vòng 72 giờ kể từ khi phát hiện.

Điều 14. Ứng cứu sự cố an toàn dữ liệu

1. Nguyên tắc ứng cứu sự cố

a) Mọi sự cố an toàn dữ liệu cá nhân, dù nhỏ hay nghiêm trọng, đều phải được phát hiện sớm, ghi nhận, báo cáo và xử lý kịp thời, nhằm giảm thiểu tác động và ngăn chặn lan truyền.

b) Việc ứng cứu sự cố phải đảm bảo tính minh bạch, có bằng chứng kỹ thuật lưu giữ đầy đủ phục vụ điều tra và xác minh nguyên nhân.

c) Mọi đơn vị, cá nhân có trách nhiệm phối hợp và không được che giấu, trì hoãn hoặc xóa dấu vết sự cố.

2. Phân loại mức độ sự cố

a) Sự cố nhẹ: rò rỉ, mất mát hoặc thay đổi dữ liệu cá nhân ở phạm vi hạn chế (dưới 10 cá nhân), chưa gây thiệt hại thực tế hoặc ảnh hưởng ngoài nội bộ.

b) Sự cố trung bình: sự cố ảnh hưởng từ 10 đến 100 cá nhân, có nguy cơ bị truy cập trái phép hoặc làm lộ thông tin nhạy cảm, nhưng chưa lan rộng ra bên ngoài Trường.

c) Sự cố nghiêm trọng: sự cố rò rỉ dữ liệu trên 100 cá nhân, bị truy cập trái phép từ bên ngoài, hoặc ảnh hưởng đến toàn bộ hệ thống lưu trữ, gây gián đoạn dịch vụ hoặc thiệt hại về uy tín, tài chính.

3. Thực hiện quy trình ứng cứu sự cố theo Quy chế An toàn thông tin và An ninh mạng của Trường theo Quyết định số 8684/QĐ-ĐHTCM ngày 10/11/2025.

4. Việc xử lý dữ liệu ngoài hệ thống thông tin của Trường phải đảm bảo mã hóa, ghi nhận nhật ký, và chỉ được thực hiện khi có ý kiến của Viện Đổi mới sáng tạo và Chuyển đổi số.

5. Báo cáo và thông báo sự cố

a) Báo cáo nội bộ: Viện Đổi mới sáng tạo và Chuyển đổi số tổng hợp, báo cáo Hiệu trưởng hoặc Phó Hiệu trưởng phụ trách trong vòng 24 giờ kể từ khi phát hiện sự cố.

b) Báo cáo cơ quan quản lý: Đối với sự cố nghiêm trọng, có nguy cơ ảnh hưởng rộng hoặc xâm phạm dữ liệu nhạy cảm, Viện Đổi mới sáng tạo và Chuyển đổi số có trách nhiệm báo cáo các cơ quan quản lý nhà nước theo Điều 22 - Nghị định số 13/2023/NĐ-CP.

c) Thông báo cho chủ thể dữ liệu: Nếu sự cố ảnh hưởng đến dữ liệu cá nhân, Trường phải thông báo cho các chủ thể bị tác động trong vòng 05 ngày làm việc kể từ khi xác định phạm vi ảnh hưởng, nêu rõ: loại dữ liệu, thời gian, nguyên nhân và biện pháp khắc phục.

6. Lưu hồ sơ và đánh giá sau sự cố

a) Mỗi sự cố phải có hồ sơ lưu trữ đầy đủ gồm: báo cáo ban đầu, nhật ký xử lý, bằng chứng kỹ thuật, biên bản họp, kết quả phục hồi và đánh giá sau cùng.

b) Viện Đổi mới sáng tạo và Chuyển đổi số có trách nhiệm tổng hợp, đánh giá định kỳ hàng năm các sự cố và đề xuất biện pháp phòng ngừa, cải thiện hệ thống kỹ thuật.

7. Các đơn vị, cá nhân liên quan phải phối hợp cung cấp đầy đủ thông tin, bằng chứng phục vụ công tác điều tra, khắc phục và rút kinh nghiệm sau sự cố.

8. Kết quả khắc phục sự cố phải được tổng hợp vào báo cáo định kỳ hằng năm về an toàn dữ liệu của Trường.

Chương IV
KIỂM TRA, GIÁM SÁT VÀ XỬ LÝ VI PHẠM

Điều 15. Kiểm tra và giám sát

1. Phạm vi và đối tượng kiểm tra

a) Bao gồm toàn bộ hệ thống thông tin, thiết bị, nền tảng số, cơ sở dữ liệu và quy trình xử lý dữ liệu cá nhân của Trường.

b) Áp dụng cho các đơn vị thuộc và trực thuộc Trường, các nhà cung cấp dịch vụ, đối tác có xử lý dữ liệu cá nhân.

2. Hình thức và tần suất

a) Kiểm tra định kỳ 06 tháng/lần và theo kế hoạch hằng năm.

b) Kiểm tra đột xuất khi có sự cố, rủi ro hoặc khi có yêu cầu của Hiệu trưởng hoặc cơ quan quản lý cấp trên.

c) Tổ chức diễn tập an toàn dữ liệu ít nhất 01 lần/năm, có thể kết hợp với kiểm tra kỹ thuật an toàn thông tin mạng.

3. Nội dung kiểm tra

a) Việc tuân thủ quy định về thu thập, xử lý, chia sẻ dữ liệu cá nhân.

b) Kiểm tra nhật ký truy cập, lưu trữ, sao lưu và tiêu hủy dữ liệu.

c) Kiểm tra hồ sơ đánh giá tác động xử lý dữ liệu và nhật ký sự cố.

d) Kiểm tra việc phân quyền truy cập, lưu trữ dữ liệu trên nền tảng đám mây, sử dụng thiết bị cá nhân trong công việc và việc lưu trữ dữ liệu trên nền tảng công cộng.

e) Đánh giá định kỳ việc thực hiện các biện pháp khắc phục sau kiểm tra và theo dõi kết quả cải thiện.

f) Việc kiểm tra có thể kết hợp với công tác đánh giá cấp độ an toàn hệ thống thông tin của Trường theo Nghị định số 85/2016/NĐ-CP.

g) Kết quả kiểm tra là căn cứ để xem xét đánh giá mức độ tuân thủ và đề xuất biện pháp khắc phục cho kỳ tiếp theo.

4. Báo cáo và lưu trữ kết quả

a) Kết quả kiểm tra được thông báo cho đơn vị được kiểm tra và lưu tại Viện tối thiểu 24 tháng. Đơn vị phải báo cáo kết quả khắc phục trong vòng 15 ngày kể từ khi nhận biên bản kiểm tra.

b) Báo cáo gửi Hiệu trưởng hoặc Phó Hiệu trưởng phụ trách trong vòng 10 ngày sau khi hoàn thành kiểm tra.

c) Hồ sơ kiểm tra được lưu tối thiểu 24 tháng tại Viện Đổi mới sáng tạo và Chuyển đổi số.

Điều 16. Xử lý vi phạm

1. Không báo cáo, che giấu hoặc xử lý sai quy trình sự cố dữ liệu cá nhân bị xem là hành vi vi phạm. Cá nhân, đơn vị vi phạm phải chịu trách nhiệm theo quy định của pháp luật và các quy định, quy chế của Trường.

2. Vi phạm quy định về bảo vệ dữ liệu cá nhân được phân loại theo mức độ ảnh hưởng như sau:

a) Vi phạm nhẹ: Hành vi vi phạm quy trình kỹ thuật hoặc thủ tục nội bộ, chưa gây thiệt hại, chưa ảnh hưởng đến quyền và lợi ích của chủ thể dữ liệu và không làm gián đoạn hoạt động của hệ thống thông tin.

b) Vi phạm trung bình: Hành vi gây lộ, mất, sai lệch hoặc làm thay đổi dữ liệu cá nhân của dưới 10 chủ thể dữ liệu, ảnh hưởng đến hoạt động nội bộ hoặc tiềm ẩn rủi ro về an toàn dữ liệu.

c) Vi phạm nghiêm trọng: Hành vi rò rỉ, mất, thay đổi hoặc công bố trái phép dữ liệu cá nhân của từ 10 chủ thể dữ liệu trở lên, hoặc gây thiệt hại về vật chất, tinh thần, quyền lợi hợp pháp của chủ thể dữ liệu hoặc ảnh hưởng đến hoạt động của hệ thống thông tin và uy tín của Nhà trường.

d) Các vi phạm khác được phân tích, đánh giá và tổng hợp theo kết quả báo cáo định kỳ hằng năm để xác định mức độ ảnh hưởng và cấp độ tuân thủ.

3. Tùy theo mức độ vi phạm, Hiệu trưởng quyết định áp dụng hình thức xử lý kỷ luật theo thẩm quyền, bao gồm: nhắc nhở, cảnh cáo, tạm đình chỉ quyền truy cập hệ thống, xử lý kỷ luật đối với viên chức, người lao động hoặc người học theo quy định hiện hành. Trường hợp hành vi vi phạm có dấu hiệu vi phạm pháp luật, Nhà trường sẽ chuyển hồ sơ đến cơ quan có thẩm quyền để xem xét, xử lý theo quy định.

4. Viện Đổi mới sáng tạo và Chuyển đổi số có trách nhiệm tổng hợp, báo cáo định kỳ các vi phạm và biện pháp xử lý cho Hiệu trưởng; lưu hồ sơ xử lý vi phạm tối thiểu 24 tháng để phục vụ kiểm tra, thanh tra nội bộ.

5. Trường hợp vi phạm nghiêm trọng quy định pháp luật về bảo vệ dữ liệu cá nhân, Hiệu trưởng hoặc đơn vị được ủy quyền có trách nhiệm báo cáo ngay cho cơ quan quản lý nhà nước có thẩm quyền.

Chương V
ĐIỀU KHOẢN THI HÀNH

Điều 17. Điều khoản thi hành

1. Quy chế Bảo vệ dữ liệu cá nhân 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. 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
MẪU BIỂU HỒ SƠ VÀ BÁO CÁO XỬ LÝ DỮ LIỆU CÁ NHÂN

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

BM/V.ĐMSTCĐS/26

TRƯỜNG ĐẠI HỌC
TÀI CHÍNH – MARKETING

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

ĐƠN VỊ: .....

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

HỒ SƠ ĐÁNH GIÁ TÁC ĐỘNG XỬ LÝ DỮ LIỆU CÁ NHÂN

1. Thông tin chung

Tên đơn vị lập hồ sơ: .....

Người phụ trách xử lý dữ liệu: .....

Chức vụ/ Đơn vị: .....

Đơn vị phụ trách kỹ thuật (nếu khác đơn vị lập hồ sơ): .....

Ngày lập hồ sơ: .....

2. Mục đích và phạm vi xử lý dữ liệu

Mục đích thu thập và xử lý: .....

Căn cứ pháp lý hoặc sự đồng ý của chủ thể dữ liệu: .....

Phạm vi dữ liệu thu thập: .....

Hình thức xử lý (thu thập, lưu trữ, chia sẻ, truyền tải, xóa: .....

.....

Thời gian lưu trữ dự kiến: .....

3. Loại dữ liệu cá nhân được xử lý

Nhóm dữ liệu	Ví dụ cụ thể
Dữ liệu cơ bản	Họ tên, CCCD, địa chỉ, email, số điện thoại, mã sinh viên,…
Dữ liệu phát sinh điện tử	Nhật ký truy cập, thông tin tài khoản LMS, lịch sử nộp bài, hồ sơ điện tử,…
Dữ liệu nhạy cảm	Dữ liệu sức khỏe, tài chính, kỷ luật, hình ảnh, video,…

4. Đánh giá rủi ro và biện pháp bảo vệ

Nội dung	Mức độ nghiêm trọng	Biện pháp phòng ngừa/ khắc phục
Rò rỉ dữ liệu cá nhân	- Nhẹ - Trung bình - Nghiêm trọng	
Truy cập trái phép	- Nhẹ - Trung bình - Nghiêm trọng	
Sử dụng sai mục đích	- Nhẹ - Trung bình - Nghiêm trọng	
Mất dữ liệu (lỗi hệ thống)	- Nhẹ - Trung bình - Nghiêm trọng	
Thiếu đồng ý của chủ thể dữ liệu	- Nhẹ - Trung bình - Nghiêm trọng	

5. Đánh giá tính hợp pháp và tuân thủ

Tiêu chí	Tính tuân thủ	Biện pháp phòng ngừa/ khắc phục
Có thông báo cho chủ thể dữ liệu trước khi thu thập	- Có - Không	
Có cơ chế rút lại sự đồng ý của chủ thể dữ liệu	- Có - Không	
Có biện pháp mã hóa, ẩn danh dữ liệu nhạy cảm	- Có - Không	
Có phân quyền truy cập hợp lý	- Có - Không	
Có lưu nhật ký truy cập hệ thống	- Có - Không	
Có đào tạo/tập huấn/tuyên truyền nội bộ định kỳ	- Có - Không	

6. Kết luận và kiến nghị

Tóm tắt kết quả đánh giá:.....

Kiến nghị bổ sung biện pháp kỹ thuật/hành chính: .....

Xác nhận của Viện ĐMSTCĐS	**Người lập hồ sơ**
(Ký, ghi rõ họ tên)	*(Ký, ghi rõ họ tên)*

BM/V.ĐMSTCĐS/27

TRƯỜNG ĐẠI HỌC
TÀI CHÍNH – MARKETING

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

ĐƠN VỊ: .....

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

BÁO CÁO SỰ CỐ VI PHẠM DỮ LIỆU CÁ NHÂN

1. Thông tin sự cố

Tên đơn vị phát hiện sự cố: .....

Người báo cáo: .....

Chức vụ/Đơn vị: .....

Thời gian phát hiện: .....giờ.....phút, ngày: .....

Thời gian xảy ra (ước tính): .....

Hệ thống/ dịch vụ bị ảnh hưởng: .....

2. Mô tả chi tiết sự cố

Loại sự cố: ☐ Truy cập trái phép ☐ Rò rỉ dữ liệu ☐ Mất dữ liệu

☐ Khai thác sai mục đích ☐ Khác: .....

Nguyên nhân ban đầu (ước tính): .....

Phạm vi ảnh hưởng (số lượng bản ghi, đối tượng): .....

.....

.....

.....

.....

Loại dữ liệu bị ảnh hưởng: .....

Mức độ nghiêm trọng: ☐ Nhẹ ☐ Trung bình ☐ Nghiêm trọng

Các biện pháp khắc phục đã thực hiện: .....

.....

.....

.....

.....

.....

.....

3. Biện pháp khắc phục và phòng ngừa

Nội dung	Thực hiện (Có/ Không)	Người chịu trách nhiệm
Cô lập sự cố và tạm ngừng truy cập hệ thống	- Có - Không	
Xác định phạm vi dữ liệu bị ảnh hưởng	- Có - Không	
Thông báo cho chủ thể dữ liệu (nếu cần)	- Có - Không	
Báo cáo Viện Đổi mới sáng tạo và Chuyển đổi số	- Có - Không	
Báo cáo cơ quan cấp trên nếu sự cố nghiêm trọng	- Có - Không	
Đề xuất cải thiện, phòng ngừa tái diễn	- Có - Không	

Thời hạn lưu trữ hồ sơ: Tối thiểu 36 tháng kể từ ngày kết thúc sự cố.

Các tài liệu giấy (bản cứng) phải được lưu trữ tại đơn vị phụ trách trong thời hạn quy định hoặc chuyển sang lưu trữ điện tử an toàn trước khi tiêu hủy./.

Xác nhận của Viện ĐMSTCĐS
(Ký, ghi rõ họ tên)

Người lập báo cáo
(Ký, ghi rõ họ tên)

BM/V.ĐMSTCĐS/28

TRƯỜNG ĐẠI HỌC
TÀI CHÍNH – MARKETING

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

ĐƠN VỊ: .....

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

BIÊN BẢN KIỂM TRA, TỰ ĐÁNH GIÁ ĐỊNH KỲ VỀ BẢO VỆ DỮ LIỆU CÁ NHÂN

I. Thông tin chung

1) Đơn vị: .....

2) Người thực hiện đánh giá:

Họ và tên: ..... Chức vụ: .....

Email: ..... Số điện thoại: .....

3) Thời kỳ đánh giá: Từ ...../...../..... đến ...../...../.....

4) Hệ thống/ quy trình có xử lý dữ liệu do cá nhân phụ trách (đánh dấu ✓):

☐ Tuyển sinh ☐ Đào tạo/LMS ☐ Khảo thí ☐ Nhân sự-tiền lương

☐ Tài chính - học phí ☐ Trang/cổng thông tin ☐ Khác: .....

5) Nhóm dữ liệu xử lý: ☐ Cơ bản ☐ Phát sinh điện tử/hồ sơ số ☐ Nhạy cảm (nêu rõ):

.....

.....

II. Tổ chức và trách nhiệm

STT	Nội dung kiểm tra / Tự đánh giá	Đã thực hiện	Chưa thực hiện	Giải trình/ Ghi chú
1	Đơn vị có phân công 01 viên chức phụ trách công tác bảo mật dữ liệu cá nhân chưa?	□	□	
2	Đơn vị có tổ chức phổ biến, tuyên truyền Quy chế an toàn thông tin cá nhân này cho toàn bộ viên chức, người lao động thuộc phạm vi quản lý chưa?	□	□	
3	Viên chức, người lao động trong đơn vị có tham dự đầy đủ các chương trình tập huấn, kiểm tra về an toàn thông tin và bảo vệ dữ liệu cá nhân do Viện ĐMST&CĐS tổ chức không?	□	□	

III. Quản lý truy cập và sử dụng dữ liệu

STT	Nội dung kiểm tra / Tự đánh giá	Đã thực hiện	Chưa thực hiện	Giải trình/ Ghi chú
1	Đơn vị có rà soát, đảm bảo việc phân quyền truy cập dữ liệu cá nhân (xem, sửa, xóa) đúng chức năng, nhiệm vụ được giao cho từng cá nhân?	□	□	
2	Đơn vị có đảm bảo 100% viên chức không chia sẻ thông tin đăng nhập, mật khẩu cá nhân cho người khác dưới bất kỳ hình thức nào không?	□	□	
3	Khi xử lý dữ liệu, đơn vị có tuân thủ nguyên tắc "Giảm thiểu dữ liệu" (chỉ thu thập/sử dụng thông tin thực sự cần thiết) không?	□	□	

IV. Lưu trữ, chia sẻ dữ liệu

STT	Nội dung kiểm tra/ Tự đánh giá	Đã thực hiện	Chưa thực hiện	Giải trình/ Ghi chú
1	Đơn vị có hành vi tự ý sao chép, lưu trữ DLCN (hồ sơ, bảng điểm, danh sách,...) ra thiết bị cá nhân hoặc nền tảng bên ngoài (Zalo, Google Drive cá nhân, email cá nhân) không? (Mục này đánh "*Đã thực hiện*" nếu KHÔNG có hành vi vi phạm)	□	□	
2	Việc chia sẻ dữ liệu nội bộ trong Trường (cho đơn vị khác) có được sự đồng ý của Trưởng đơn vị và ghi nhận mục đích rõ ràng không?	□	□	
3	Khi xử lý dữ liệu, đơn vị có tuân thủ nguyên tắc "*Giảm thiểu dữ liệu*" (chỉ thu thập/sử dụng thông tin thực sự cần thiết) không?	□	□	
4	Các tài liệu giấy (bản cứng) chứa dữ liệu cá nhân khi không còn sử dụng có được tiêu hủy an toàn (ví dụ: qua máy hủy tài liệu) thay vì vứt vào sọt rác thông thường không?	□	□	

V. Giám sát và ứng cứu sự cố

STT	Nội dung kiểm tra/ Tự đánh giá	Đã thực hiện	Chưa thực hiện	Giải trình/ Ghi chú
1	Mọi cá nhân trong đơn vị có nắm rõ quy trình: phải "*Báo cáo ngay*" cho Viện ĐMST&CĐS khi phát hiện sự cố/nghi ngờ rò rỉ dữ liệu (ví dụ: gửi nhầm email, mã hóa dữ liệu, quên mật khẩu tài khoản,...)?	□	□	
2	Đơn vị có hành vi nào che giấu, chậm báo cáo hoặc tự ý xóa dấu vết khi phát hiện sự cố không? * (Mục này đánh "*Đã thực hiện*" nếu KHÔNG có hành vi vi phạm)	□	□	
3	Đơn vị có thực hiện báo cáo định kỳ 06 tháng/lần về tình hình bảo vệ dữ liệu cá nhân cho Viện ĐMST&CĐS theo quy định không?	□	□	

VI. Đánh giá chung và cam kết

Các rủi ro/khó khăn chính trong công tác bảo vệ dữ liệu cá nhân tại đơn vị:

.....

.....

.....

Đề xuất/kiến nghị (với Viện ĐMST&CĐS hoặc Ban Giám hiệu):

.....

.....

.....

Đơn vị cam kết các thông tin trên là đúng sự thật, phản ánh chính xác tình hình tuân thủ tại đơn vị và chịu trách nhiệm về kết quả tự đánh giá này.

Người lập biểu	**Trưởng đơn vị**
(Ký, ghi rõ họ tên)	*(Ký, ghi rõ họ tên)*

Ghi chú: Trưởng đơn vị phối hợp với viên chức phụ trách bảo mật dữ liệu (nếu có) rà soát và đánh dấu vào ô tương ứng. Đối với các mục "*Chưa thực hiện*", vui lòng nêu lý do hoặc kế hoạch khắc phục ở cột "*Giải trình/Ghi chú*".