

Số: 8016 /KH-SGDĐT

Thành phố Hồ Chí Minh, ngày 06 tháng 8 năm 2026

KẾ HOẠCH

Triển khai thực hiện bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong ngành Giáo dục và Đào tạo Thành phố Hồ Chí Minh giai đoạn 2026 - 2030

Căn cứ Luật Dữ liệu năm 2024;

Căn cứ Luật Bảo vệ dữ liệu cá nhân năm 2025;

Căn cứ Luật An ninh mạng năm 2025;

Căn cứ Chỉ thị số 57-CT/TW ngày 31 tháng 12 năm 2025 của Ban Bí thư về tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị;

Căn cứ Kế hoạch số 04-KH/BCĐTW ngày 05 tháng 01 năm 2026 của Ban Chỉ đạo Trung ương về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số về bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong hệ thống chính trị;

Căn cứ Kế hoạch số 34-KH/BCĐTP ngày 05 tháng 5 năm 2026 của Ban Chỉ đạo về phát triển khoa học, công nghệ, đổi mới sáng tạo, chuyển đổi số Thành phố Hồ Chí Minh triển khai thực hiện bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong hệ thống chính trị trên địa bàn Thành phố;

Căn cứ Kế hoạch số 191/KH-TBANM ngày 15 tháng 5 năm 2026 của Tiểu ban An ninh mạng Thành phố Hồ Chí Minh về bảo đảm an ninh mạng trong toàn hệ thống chính trị Thành phố Hồ Chí Minh năm 2026;

Căn cứ chức năng, nhiệm vụ và quyền hạn của Sở Giáo dục và Đào tạo Thành phố Hồ Chí Minh;

Sở Giáo dục và Đào tạo Thành phố Hồ Chí Minh xây dựng Kế hoạch triển khai thực hiện bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong ngành Giáo dục và Đào tạo Thành phố Hồ Chí Minh giai đoạn 2026 - 2030 với các nội dung cụ thể sau:

I. MỤC TIÊU, YÊU CẦU

1. Mục tiêu chung

- Bảo đảm an ninh mạng tuyệt đối cho các hệ thống thông tin, cơ sở dữ liệu (CSDL) ngành Giáo dục và Đào tạo (GDĐT) Thành phố, phục vụ có hiệu quả công cuộc chuyển đổi số, xây dựng đô thị thông minh và giáo dục thông minh.

- Chủ động phòng ngừa, phát hiện kịp thời và ngăn chặn hiệu quả các loại phần mềm độc hại, mã độc tấn công, các nguy cơ đe dọa an ninh mạng; sẵn sàng phương án ứng phó và xử lý nhanh chóng các sự cố an ninh mạng trong ngành.

- Nâng cao nhận thức, năng lực và kỹ năng phòng chống mất an toàn thông tin, bảo vệ dữ liệu cá nhân cho đội ngũ cán bộ quản lý, giáo viên, nhân viên, học sinh, sinh viên trong toàn ngành Giáo dục và Đào tạo Thành phố.

2. Mục tiêu cụ thể

a) Mục tiêu trọng tâm năm 2026

- Các hệ thống thông tin của Sở Giáo dục và Đào tạo, và các cơ sở giáo dục trực thuộc được đưa vào danh mục giám sát, bảo đảm an ninh mạng theo đúng quy định.

- 100% hệ thống thông tin đang vận hành của ngành Giáo dục và Đào tạo Thành phố hoàn thành việc xây dựng, cập nhật phương án bảo đảm an ninh mạng và hồ sơ đề xuất cấp độ hệ thống thông tin theo đúng quy định của Luật An ninh mạng năm 2025.

- 100% máy chủ, máy trạm và thiết bị đầu cuối của ngành Giáo dục phục vụ công tác điều hành, quản trị dữ liệu được cài đặt và duy trì hoạt động giải pháp phòng chống mã độc tập trung, có kết nối chia sẻ thông tin giám sát về Trung tâm An ninh mạng Thành phố.

- 100% cơ quan Sở và các đơn vị giáo dục trực thuộc hoàn thành việc triển khai mô hình bảo đảm an toàn thông tin chuyên nghiệp “4 lớp” bao gồm: (1) Lực lượng tại chỗ chịu trách nhiệm vận hành, giám sát và ứng cứu ban đầu khi sự cố xảy ra; (2) Hệ thống hoặc dịch vụ giám sát 24/7, giúp phát hiện sớm các nguy cơ; (3) Đơn vị độc lập thực hiện kiểm tra, đánh giá định kỳ để đảm bảo khách quan và minh bạch; (4) Kết nối, chia sẻ thông tin với hệ thống giám sát an ninh mạng quốc gia, bảo đảm sự phối hợp liên thông trên phạm vi toàn quốc.

- Tổ chức tuyên truyền, phổ biến pháp luật, nâng cao nhận thức về an ninh mạng cho cán bộ công chức, viên chức và người dùng Internet trong toàn ngành GDĐT Thành phố.

- Tổ chức hoặc phối hợp tổ chức ít nhất 01 đợt diễn tập thực chiến ứng phó sự cố an ninh mạng cấp ngành hoặc tham gia diễn tập cấp Thành phố trong năm 2026.

b) Định hướng giai đoạn 2026 – 2030

- Đảm bảo an ninh dữ liệu tuyệt đối cho các hệ thống thông tin dùng chung của ngành Giáo dục Thành phố, không để xảy ra sự cố lộ lọt thông tin diện rộng.

- Các chương trình, đề án, dự án đầu tư ứng dụng công nghệ thông tin sử dụng nguồn ngân sách phải bố trí kinh phí tối thiểu 15% cho công tác bảo đảm an ninh mạng và an toàn thông tin.

- Triển khai các chương trình đào tạo, bồi dưỡng, phổ biến kiến thức an ninh mạng trên nền tảng “Bình dân học vụ số”

- Hoàn thành việc tích hợp nội dung giảng dạy kiến thức và kỹ năng an ninh mạng, kỹ năng tự bảo vệ trên không gian mạng vào chương trình giáo dục phổ thông (từ Trung học cơ sở đến Trung học phổ thông), giáo dục thường xuyên và các cơ sở giáo dục nghề nghiệp trực thuộc.

3. Yêu cầu

- Kế hoạch phải được triển khai đồng bộ, nghiêm túc, thực chất và thống nhất trong toàn ngành Giáo dục và Đào tạo Thành phố; phân công trách nhiệm rõ ràng, có tiến độ, sản phẩm đo lường cụ thể, tránh hình thức và dàn trải.

- Gắn chặt trách nhiệm cá nhân của người đứng đầu các cơ quan quản lý giáo dục, người đứng đầu các đơn vị trực thuộc với kết quả bảo đảm an ninh mạng của đơn vị. Kết quả thực hiện công tác bảo mật an toàn an ninh thông tin, an ninh mạng được coi là tiêu chí xếp loại thi đua, khen thưởng và đánh giá năng lực cán bộ quản lý hàng năm.

II. NHIỆM VỤ VÀ GIẢI PHÁP TRỌNG TÂM

1. Phổ biến, quán triệt nâng cao nhận thức pháp luật và kỹ năng an ninh mạng

- Tổ chức phổ biến sâu rộng các văn bản quy phạm pháp luật, chỉ đạo của Đảng, Nhà nước và Thành phố về an ninh mạng (như Luật An ninh mạng 2025, Chỉ thị 57-CT/TW) đến 100% cán bộ quản lý, giáo viên, nhân viên, học sinh, sinh viên.

- Phát động phong trào thi đua “Dân vận khéo trên không gian mạng” trong học đường, phát huy vai trò tiên phong của giáo viên và học sinh trong việc xây dựng môi trường mạng văn hóa, an toàn.

- Biên soạn và phân phối các bộ tài liệu, cẩm nang hướng dẫn trực quan, sinh động (nhận diện lừa đảo trực tuyến, bảo mật mật khẩu, bảo vệ thông tin cá nhân) cho học sinh các cấp và phụ huynh.

2. Đổi mới chương trình, nội dung giáo dục về an toàn, an ninh mạng

- Sở Giáo dục và Đào tạo chủ trì, phối hợp với các chuyên gia an ninh mạng biên soạn, lồng ghép nội dung giáo dục kiến thức, kỹ năng số và an toàn thông tin cơ bản vào chương trình giáo dục phổ thông (đặc biệt là cấp Trung học cơ sở và Trung học phổ thông), giáo dục thường xuyên, các chương trình hướng nghiệp.

- Đa dạng hóa hình thức truyền tải, tuyên truyền nội dung giáo dục về an toàn, an ninh mạng qua các hoạt động ngoại khóa, chuyên đề sinh hoạt dưới cờ, xây dựng các khóa học số ngắn hạn trên nền tảng học tập trực tuyến dùng chung của ngành.

3. Đào tạo, phát triển nguồn nhân lực chuyên trách an ninh mạng

- Sở Giáo dục và Đào tạo chủ trì, phối hợp với Tiểu ban An ninh mạng Thành phố, Công an Thành phố xây dựng và tổ chức thực hiện các chương trình đào tạo chuyên sâu, bồi dưỡng định kỳ và huấn luyện thực tế về công tác bảo mật, an toàn thông tin và an ninh mạng cho đội ngũ cán bộ chuyên trách, công chức, viên chức kiêm nhiệm công nghệ thông tin tại cơ quan Sở, bộ phận chuyên trách giáo dục tại Ủy ban nhân dân phường/xã/đặc khu và các cơ sở giáo dục trực thuộc. Nội dung tập trung nâng cao năng lực giám sát hệ thống, nhận diện sớm các mối đe dọa, kỹ năng ứng phó sự cố khẩn cấp, phương pháp bóc tách mã độc hại và bảo vệ an toàn dữ liệu ngành. Định kỳ tổ chức các chương trình diễn tập thực chiến phòng ngừa sự cố mạng thường niên.

- Chủ động thiết lập và thúc đẩy hiệu quả mô hình liên kết chặt chẽ “Nhà nước – Nhà trường – Doanh nghiệp” trong công tác đào tạo, bồi dưỡng và huấn luyện an ninh mạng thực chiến. Phối hợp với các trường Đại học, Cao đẳng, cơ sở giáo dục nghề nghiệp trực thuộc có đào tạo chuyên ngành công nghệ thông tin và an toàn thông tin để triển khai các chương trình thực tập, học tập thực tế và huấn luyện thực hành trực tiếp tại các doanh nghiệp an ninh mạng hàng đầu. Kết nối hiệu quả với Mạng lưới liên kết các chuyên gia an ninh mạng để huy động nguồn lực trí tuệ, sẵn sàng hỗ trợ kỹ thuật khi cần thiết.

- Tiến hành rà soát, kiện toàn và tăng cường nguồn nhân lực chuyên trách bảo đảm an ninh mạng tại cơ quan Sở và các trường THPT trực thuộc.

4. Bảo đảm nguồn lực tài chính, ngân sách cho an ninh mạng

- Quy định bắt buộc lồng ghép hạng mục bảo đảm an toàn thông tin, an ninh mạng trong mọi chương trình, đề án, dự án ứng dụng công nghệ thông tin và chuyển đổi số trong ngành Giáo dục.

- Bảo đảm tỷ lệ kinh phí dành riêng cho các giải pháp, dịch vụ bảo mật đạt tối thiểu 15% tổng mức đầu tư của đề án, dự án đầu tư công nghệ thông tin, ứng dụng số của các đơn vị.

5. Tăng cường trách nhiệm của Người đứng đầu và triển khai Chương trình đánh giá tín nhiệm mạng

- Đề cao vai trò lãnh đạo, chỉ đạo, kiểm tra và đôn đốc thực hiện công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu của người đứng đầu các cơ quan quản lý và cơ sở giáo dục. Người đứng đầu đơn vị chịu trách nhiệm trực tiếp và toàn diện nếu để xảy ra sự cố an ninh mạng nghiêm trọng, đặc biệt là lộ, lọt bí mật nhà nước do yếu tố chủ quan, thiếu trách nhiệm hoặc không tuân thủ quy định.

- Chủ trì phối hợp triển khai chương trình đánh giá dán nhãn “Tín nhiệm mạng” đối với các cổng thông tin, cổng hành chính công, và các kênh tương tác

của tổ chức, cá nhân có ảnh hưởng trên không gian mạng thuộc quản lý ngành nhằm bảo vệ học sinh, giáo viên và củng cố niềm tin công chúng.

6. Chủ trì xây dựng phương án ứng cứu sự cố và triển khai giải pháp giám sát, phản ứng nhanh

- Chủ trì, phối hợp với Công an Thành phố (Tiểu ban An ninh mạng) xây dựng phương án ứng cứu sự cố an ninh mạng chi tiết cho hệ thống thông tin thuộc phạm vi quản lý; triển khai tổng thể các giải pháp giám sát chủ động, bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu và ứng phó xử lý nhanh sự cố đột xuất.

- Thực hiện kết nối, chia sẻ thông tin dữ liệu giám sát an ninh mạng 24/7 từ các hệ thống thông tin dùng chung quan trọng của ngành về Trung tâm An ninh mạng Thành phố (do Công an Thành phố vận hành) để tối ưu hóa khả năng ứng phó từ xa.

III. TỔ CHỨC THỰC HIỆN

1. Phân công trách nhiệm các đơn vị thuộc Sở và địa phương

a) Văn phòng Sở

- Chủ trì tham mưu Ban Giám đốc Sở trong công tác chỉ đạo, hướng dẫn, kiểm tra và đôn đốc việc thực hiện Kế hoạch này đối với tất cả các phòng ban, cơ sở giáo dục trực thuộc.

- Đầu mối phối hợp chặt chẽ với Công an Thành phố (Tiểu ban An ninh mạng) xây dựng phương án ứng cứu sự cố tổng thể của ngành; kết nối chia sẻ dữ liệu giám sát 24/7 về Trung tâm An ninh mạng Thành phố.

- Chủ trì triển khai chương trình đánh giá dán nhãn “Tín nhiệm mạng” đối với hệ thống dịch vụ hành chính công, trang thông tin điện tử của Sở và các đơn vị thành viên.

- Chịu trách nhiệm trực tiếp bảo vệ an toàn hệ thống hạ tầng mạng đặt tại Sở. Đầu mối tổng hợp, xây dựng báo cáo định kỳ.

b) Phòng Giáo dục Phổ thông

- Chủ trì tham mưu xây dựng tài liệu, tích hợp nội dung giảng dạy kiến thức và kỹ năng an ninh mạng, kỹ năng tự bảo vệ trên không gian mạng vào chương trình chính khóa môn Tin học, các hoạt động giáo dục trải nghiệm, hướng nghiệp cho toàn thể học sinh các cấp phổ thông (Tiểu học, Trung học cơ sở, Trung học phổ thông) trên địa bàn Thành phố.

- Theo dõi, giám sát và đôn đốc các cơ sở giáo dục phổ thông triển khai thực hiện giảng dạy và phổ biến an ninh mạng học đường đạt hiệu quả thực chất, tránh hình thức.

c) Phòng Giáo dục Mầm non và Phòng Giáo dục Thường xuyên Nghề nghiệp và Đại học

- Chỉ đạo lồng ghép tuyên truyền quy tắc ứng xử văn minh và an toàn trên không gian mạng phù hợp với lứa tuổi mầm non và học viên.
- Đôn đốc các cơ sở giáo dục mầm non, trung tâm giáo dục thường xuyên trực thuộc thực hiện nghiêm túc việc rà soát lỗ hổng kỹ thuật, bảo vệ dữ liệu thông tin trẻ em và người học.

d) Ủy ban nhân dân các phường, xã, đặc khu

- Trực tiếp lãnh đạo, chỉ đạo, đôn đốc và giám sát công tác bảo đảm an ninh mạng, bảo mật thông tin và an toàn cơ sở dữ liệu đối với các trường mầm non, trường tiểu học, và trường trung học cơ sở thuộc thẩm quyền quản lý trên địa bàn.
- Phối hợp chặt chẽ với Sở Giáo dục và Đào tạo, cơ quan Công an địa phương tiến hành rà quét, khắc phục điểm yếu bảo mật kỹ thuật tại các trường học trực thuộc địa bàn phụ trách; đưa kết quả thực hiện bảo đảm an ninh mạng thành tiêu chí xếp loại, đánh giá thi đua và mức độ hoàn thành nhiệm vụ hàng năm của người đứng đầu các đơn vị giáo dục cấp xã.
- Cân đối, bố trí ngân sách địa phương đảm bảo kinh phí chi cho an toàn, an ninh mạng đạt tối thiểu 15% trong tổng kinh phí triển khai đề án, dự án, chương trình, kế hoạch đầu tư, ứng dụng, phát triển công nghệ thông tin, bảo đảm hiệu quả, đúng quy định, tránh lãng phí.

e) Hiệu trưởng các trường THPT và thủ trưởng các đơn vị trực thuộc Sở

- Chịu trách nhiệm trực tiếp và toàn diện trước Giám đốc Sở Giáo dục và Đào tạo về công tác bảo mật, an toàn thông tin tại đơn vị mình phụ trách. Nếu để xảy ra sự cố nghiêm trọng hoặc lộ lọt dữ liệu do yếu tố chủ quan sẽ bị xử lý kỷ luật nghiêm theo quy định.
- Hoàn thành việc rà soát lỗ hổng, khắc phục điểm yếu và triển khai mô hình phòng thủ “4 lớp”. Xây dựng phương án ứng phó sự cố nội bộ của trường.
- Đưa kết quả bảo đảm an ninh thông tin vào quy trình đánh giá, xếp loại công chức, viên chức dưới quyền quản lý hàng năm.

2. Chế độ thông tin, báo cáo

a) Báo cáo định kỳ hằng tháng

Các đơn vị thuộc Sở, Ủy ban nhân dân các phường, xã, đặc khu và các cơ sở giáo dục trực thuộc thực hiện cập nhật kết quả triển khai định kỳ, báo cáo về Văn

phòng Sở Giáo dục và Đào tạo trước ngày 15 hằng tháng qua link: <https://forms.gle/2bXDdfTGh9gDBoAy6>. Văn phòng Sở chịu trách nhiệm tổng hợp báo cáo toàn ngành để tham mưu Giám đốc Sở ký duyệt gửi Thường trực Ban Chỉ đạo Thành phố, Công an Thành phố trước ngày 18 hằng tháng.

b) Báo cáo đột xuất (Báo cáo sự cố khẩn cấp)

- Khi phát hiện sự cố tấn công mạng nghiêm trọng (như bị mã độc mã hóa dữ liệu tổng tiền, tấn công từ chối dịch vụ), phá hoại hệ thống hoặc có dấu hiệu lộ lọt bí mật nhà nước, rò rỉ cơ sở dữ liệu cá nhân của người học và nhân sự, đơn vị quản lý trực tiếp hệ thống phải thực hiện lập tức biện pháp cô lập kỹ thuật ban đầu tại chỗ để bảo vệ hệ thống.

- Thực hiện báo cáo khẩn cấp bằng văn bản (hoặc thông qua hệ thống báo cáo điện tử nhanh nhất) gửi về Sở Giáo dục và Đào tạo (qua Văn phòng Sở) và Công an Thành phố (Tiểu ban An ninh mạng) trong vòng 24 giờ kể từ khi phát hiện sự cố để phối hợp kỹ thuật phản ứng khẩn cấp và bóc tách mã độc.

- Nội dung báo cáo khẩn cấp phải nêu rõ: thời điểm phát hiện sự cố, mô tả sơ bộ hiện tượng và hành vi tấn công, hệ thống thông tin bị ảnh hưởng, đánh giá thiệt hại ban đầu, các biện pháp cô lập kỹ thuật đã xử lý tại chỗ và các đề xuất, kiến nghị hỗ trợ khẩn cấp từ cơ quan chuyên trách (nếu có).

Trên đây là Kế hoạch Triển khai thực hiện bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong ngành Giáo dục và Đào tạo Thành phố Hồ Chí Minh giai đoạn 2026 - 2030. Sở Giáo dục và Đào tạo đề nghị các các phòng ban chuyên môn và Thủ trưởng các cơ sở giáo dục nghiêm túc, khẩn trương triển khai thực hiện./.

Nơi nhận:

- Công an Thành phố (Tiểu ban ANM);
- UBND xã, phường, đặc khu (để phối hợp);
- Các phòng thuộc Sở (để thực hiện);
- Các cơ sở giáo dục (để thực hiện);
- Lưu: VT, VP (Tùng).

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Nguyễn Bảo Quốc