

Số: 285/KH-PEK

Thành phố Hồ Chí Minh, ngày 04 tháng 9 năm 2026

KẾ HOẠCH

Triển khai thực hiện bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu 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 Kế hoạch của Sở Giáo dục và Đào tạo Thành phố Hồ Chí Minh về 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 tình hình thực tế, trường Trung-Tiểu học Pétrus Ký xây dựng Kế hoạch triển khai thực hiện bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu giai đoạn 2026-2030 cụ thể như sau:

I. MỤC TIÊU, YÊU CẦU

1. Mục tiêu chung

- Bảo đảm an toàn, an ninh đối với hệ thống thông tin, hạ tầng mạng, cơ sở dữ liệu, tài khoản và các nền tảng số thuộc phạm vi quản lý, sử dụng của nhà trường; phục vụ ổn định hoạt động quản trị, dạy học, kiểm tra đánh giá, cung cấp thông tin và chuyển đổi số.

- Chủ động phòng ngừa, phát hiện sớm, ngăn chặn và xử lý kịp thời nguy cơ mất an toàn thông tin, phần mềm độc hại, hành vi truy cập trái phép, lừa đảo trực tuyến và nguy cơ rò rỉ dữ liệu; có phương án ứng phó khi xảy ra sự cố.

- Nâng cao nhận thức, trách nhiệm và kỹ năng tự bảo vệ trên không gian mạng cho cán bộ quản lý, giáo viên, nhân viên và học sinh; tăng cường bảo vệ dữ liệu cá nhân của người học, cha mẹ học sinh và nhân sự nhà trường.

2. Mục tiêu cụ thể

a) Trong năm 2026

- Rà soát đầy đủ danh mục hệ thống thông tin, phần mềm, cơ sở dữ liệu, máy chủ, máy trạm, thiết bị đầu cuối và hạ tầng mạng do trường quản lý hoặc trực tiếp sử dụng; xác định đầu mối quản trị và trách nhiệm đối với từng hệ thống.

- Hoàn thành rà soát điểm yếu, lỗ hổng và xây dựng phương án bảo đảm an ninh mạng, phương án ứng phó sự cố nội bộ đối với các hệ thống quan trọng của trường; đối với hệ thống thuộc diện phải thực hiện hồ sơ cấp độ an toàn/an ninh thông tin theo quy định, thực hiện hoặc phối hợp đơn vị cung cấp hoàn thiện hồ sơ.

- 100% máy chủ, máy trạm và thiết bị đầu cuối phục vụ quản trị, xử lý dữ liệu của nhà trường được cài đặt, duy trì giải pháp phòng chống mã độc và cập nhật an toàn phù hợp; các tài khoản quản trị được kiểm soát, phân quyền theo nhiệm vụ.

- Triển khai mô hình bảo đảm an toàn thông tin “4 lớp” phù hợp điều kiện của trường: lực lượng tại chỗ; hệ thống hoặc dịch vụ giám sát; kiểm tra, đánh giá độc lập định kỳ; phối hợp, chia sẻ thông tin với Sở Giáo dục và Đào tạo và cơ quan chuyên trách khi được yêu cầu.

- Tổ chức tuyên truyền, phổ biến kiến thức và kỹ năng an ninh mạng đến 100% cán bộ quản lý, giáo viên, nhân viên và học sinh bằng hình thức phù hợp; tham gia các lớp tập huấn, diễn tập do Sở Giáo dục và Đào tạo, Thành phố hoặc cơ quan có thẩm quyền tổ chức khi được triệu tập.

b) Giai đoạn 2027 - 2030

- Duy trì, cập nhật thường xuyên danh mục tài sản số, hệ thống thông tin và dữ liệu; kiểm tra định kỳ, kịp thời khắc phục điểm yếu bảo mật phát sinh.

- Không để xảy ra sự cố lộ, lọt dữ liệu diện rộng do nguyên nhân chủ quan; bảo đảm dữ liệu được quản lý, khai thác đúng phạm vi, đúng mục đích và đúng thẩm quyền.

- Duy trì mô hình “4 lớp”, nâng cao khả năng giám sát, phát hiện và phản ứng nhanh; tổ chức hoặc lồng ghép hoạt động diễn tập, xử lý tình huống an ninh mạng phù hợp với môi trường nhà trường.

- Thực hiện lồng ghép giáo dục kiến thức, kỹ năng an toàn, an ninh mạng và kỹ năng tự bảo vệ trên không gian mạng trong môn Tin học, Hoạt động trải nghiệm - hướng nghiệp, sinh hoạt lớp, sinh hoạt dưới cờ và các chuyên đề theo hướng dẫn của ngành, phù hợp từng cấp học.

3. Yêu cầu

- Triển khai đồng bộ, thiết thực, gắn với hoạt động quản trị và dạy học; phân công rõ người, rõ việc, rõ trách nhiệm, rõ thời gian và sản phẩm; không thực hiện hình thức.

- Hiệu trưởng chịu trách nhiệm chỉ đạo chung; người được giao quản trị hệ thống, tài

khoản, dữ liệu phải chịu trách nhiệm trong phạm vi nhiệm vụ được phân công.

- Tuân thủ pháp luật về an ninh mạng, dữ liệu và bảo vệ dữ liệu cá nhân; các biện pháp kỹ thuật phải phù hợp quy mô, tính chất hệ thống của cơ sở giáo dục ngoài công lập và điều kiện thực tế của nhà trường.

- Không tự ý triển khai các cơ chế giám sát, kết nối hoặc thủ tục thuộc thẩm quyền cơ quan nhà nước. Nhà trường thực hiện kết nối, chia sẻ thông tin, báo cáo và phối hợp kỹ thuật theo hướng dẫn của Sở Giáo dục và Đào tạo và cơ quan chuyên trách.

II. PHẠM VI, ĐỐI TƯỢNG THỰC HIỆN

1. Phạm vi

Kế hoạch áp dụng đối với hệ thống thông tin, website/cổng thông tin, hệ thống quản lý nhà trường, cơ sở dữ liệu học sinh và nhân sự, nền tảng dạy học trực tuyến, kho dữ liệu/tài liệu số, hệ thống thư điện tử và tài khoản công vụ của trường, hạ tầng mạng, máy chủ, máy trạm, thiết bị đầu cuối, camera và các hệ thống số khác do trường quản lý hoặc khai thác phục vụ hoạt động giáo dục.

2. Đối tượng

Ban Giám hiệu; Ban Điều hành các cấp học/cơ sở; bộ phận CNTT; Văn phòng; các tổ chuyên môn; giáo viên chủ nhiệm; giáo viên Tin học, giáo viên Hoạt động trải nghiệm - hướng nghiệp; Đoàn Thanh niên, Đội Thiếu niên; các bộ phận có khai thác, xử lý dữ liệu và toàn thể cán bộ, giáo viên, nhân viên, học sinh. Đối tác cung cấp nền tảng, phần mềm, hạ tầng tham gia ở vai trò phối hợp theo hợp đồng và yêu cầu bảo mật của nhà trường.

III. NHIỆM VỤ VÀ GIẢI PHÁP TRỌNG TÂM

1. Tuyên truyền, phổ biến nâng cao nhận thức, kỹ năng an ninh mạng

- Tổ chức phổ biến các quy định, chỉ đạo của Trung ương, Thành phố và ngành Giáo dục về an ninh mạng, bảo mật thông tin, an ninh dữ liệu và bảo vệ dữ liệu cá nhân đến cán bộ, giáo viên, nhân viên và học sinh.

- Tuyên truyền, hướng dẫn nhận diện lừa đảo trực tuyến, bảo vệ tài khoản, mật khẩu, dữ liệu cá nhân; sử dụng mạng xã hội và nền tảng số an toàn, có trách nhiệm; chú trọng các tình huống thường gặp đối với học sinh và cha mẹ học sinh.

- Sử dụng các kênh truyền thông của trường, sinh hoạt lớp, sinh hoạt dưới cờ, chuyên đề, hoạt động Đoàn - Đội và các nền tảng học tập để tuyên truyền thường xuyên; phối hợp cung cấp tài liệu hướng dẫn cho cha mẹ học sinh khi cần thiết.

2. Lồng ghép giáo dục an toàn, an ninh mạng trong hoạt động giáo dục

- Tổ chuyên môn và giáo viên căn cứ hướng dẫn của ngành để lồng ghép kiến thức, kỹ năng số, an toàn thông tin và kỹ năng tự bảo vệ trên không gian mạng vào môn Tin học, Hoạt động trải nghiệm - hướng nghiệp và các hoạt động giáo dục phù hợp.

- Ưu tiên cấp THCS và THPT đối với nội dung nhận diện nguy cơ, bảo vệ tài khoản, dữ liệu cá nhân, ứng xử văn minh và xử lý tình huống mất an toàn trên môi trường số; cấp Tiểu học thực hiện nội dung phù hợp lứa tuổi.

- Khuyến khích tổ chức chuyên đề, tình huống thực hành, cuộc thi hoặc hoạt động

trải nghiệm có nội dung an toàn số; không tổ chức các hoạt động kỹ thuật có nguy cơ ảnh hưởng hệ thống thật của nhà trường.

3. Rà soát hệ thống, hạ tầng, dữ liệu

- Bộ phận CNTT lập và cập nhật danh mục các hệ thống, phần mềm, cơ sở dữ liệu, máy chủ, máy trạm, thiết bị mạng và tài khoản quản trị; xác định đơn vị/cá nhân phụ trách, mục đích sử dụng và phạm vi dữ liệu xử lý.

- Rà soát cấu hình, tài khoản, phân quyền, mật khẩu quản trị, phần mềm bảo vệ, phiên bản hệ điều hành/phần mềm và các điểm yếu có thể gây mất an toàn; khắc phục kịp thời các nguy cơ phát hiện được.

- Đối với hệ thống do nhà cung cấp bên ngoài vận hành, yêu cầu đầu mỗi kỹ thuật phối hợp cung cấp thông tin cần thiết, khắc phục lỗi hỏng, bảo đảm tính liên tục và tuân thủ yêu cầu bảo mật theo hợp đồng và quy định của pháp luật.

4. Tổ chức mô hình bảo đảm an toàn thông tin “4 lớp”

- Lớp 1-lực lượng tại chỗ: bộ phận CNTT và nhân sự được giao quản trị hệ thống thực hiện vận hành, theo dõi, xử lý ban đầu và báo cáo sự cố.

- Lớp 2-giám sát, phát hiện: khai thác giải pháp kỹ thuật hoặc dịch vụ giám sát phù hợp đối với hệ thống quan trọng; bảo đảm có khả năng ghi nhận, cảnh báo và hỗ trợ xử lý khi xuất hiện dấu hiệu bất thường.

- Lớp 3-kiểm tra độc lập: định kỳ hoặc khi cần thiết, phối hợp đơn vị có năng lực để rà soát, đánh giá an toàn thông tin, lỗ hổng và kiến nghị khắc phục.

- Lớp 4-phối hợp liên thông: thực hiện kết nối, chia sẻ thông tin, tiếp nhận cảnh báo và phối hợp ứng cứu với Sở Giáo dục và Đào tạo, cơ quan Công an và cơ quan chuyên trách theo yêu cầu, hướng dẫn và thẩm quyền.

5. Phòng, chống mã độc, bảo vệ thiết bị đầu cuối

- Cài đặt và duy trì giải pháp phòng, chống mã độc cho máy chủ, máy trạm và thiết bị đầu cuối phục vụ quản trị, lưu trữ, khai thác dữ liệu; bảo đảm cập nhật thường xuyên và xử lý cảnh báo phát sinh.

- Không cài đặt phần mềm không rõ nguồn gốc, phần mềm bẻ khóa hoặc công cụ không phục vụ nhiệm vụ trên thiết bị quản trị của trường; hạn chế sử dụng thiết bị lưu trữ không được kiểm soát đối với máy có dữ liệu quan trọng.

- Khi có cảnh báo mã độc hoặc dấu hiệu bị tấn công, thực hiện cô lập kỹ thuật ban đầu, giữ nguyên thông tin cần thiết phục vụ xác minh và báo ngay đầu mối phụ trách.

6. Quản lý tài khoản, phân quyền, bảo mật dữ liệu

- Thực hiện cấp, thay đổi, thu hồi tài khoản theo vị trí việc làm và nhiệm vụ; không dùng chung tài khoản quản trị; rà soát định kỳ các tài khoản không còn nhu cầu sử dụng.

- Hạn chế tối đa việc tải, sao chép, chia sẻ dữ liệu học sinh, nhân sự và dữ liệu nội bộ ra ngoài hệ thống được phép; chỉ cung cấp dữ liệu khi có căn cứ, đúng mục đích và đúng thẩm quyền.

- Các bộ phận thu thập và sử dụng dữ liệu cá nhân phải bảo đảm đúng phạm vi cần thiết cho hoạt động giáo dục, quản trị nhà trường; chịu trách nhiệm bảo mật hồ sơ, danh sách và dữ liệu được giao quản lý.

7. Xây dựng phương án ứng phó sự cố an ninh mạng

- Xây dựng đầu mối tiếp nhận thông tin sự cố, quy trình báo cáo nội bộ, cô lập kỹ thuật ban đầu, phối hợp khắc phục và khôi phục hoạt động; xác định rõ người quyết định và người trực tiếp xử lý.

- Các tình huống trọng tâm gồm: mã độc mã hóa dữ liệu tổng tiền, tấn công làm gián đoạn dịch vụ, truy cập trái phép, mất quyền kiểm soát tài khoản, rò rỉ dữ liệu cá nhân của học sinh/nhân sự hoặc dấu hiệu lộ, lọt thông tin thuộc diện bảo vệ.

- Hằng năm tổ chức hoặc lồng ghép ít nhất 01 hoạt động diễn tập mô phỏng/tình huống xử lý sự cố trong phạm vi nhà trường; tham gia diễn tập cấp ngành, cấp Thành phố khi được triệu tập.

8. Đào tạo nhân sự phụ trách CNTT

- Cử cán bộ phụ trách CNTT tham gia đầy đủ các chương trình tập huấn, bồi dưỡng, diễn tập về an ninh mạng, an toàn thông tin do Sở Giáo dục và Đào tạo, Công an Thành phố và cơ quan chuyên môn tổ chức. Tổ chức chia sẻ, cập nhật nội bộ về cảnh báo an ninh mạng, phương thức tấn công mới, quy trình xử lý sự cố và những lỗi thường gặp trong sử dụng hệ thống, tài khoản và dữ liệu.

IV. TIẾN ĐỘ THỰC HIỆN GIAI ĐOẠN 2026 - 2030

TT	Thời gian	Nhiệm vụ trọng tâm	Đầu mối	Kết quả	Kiểm tra
1	09-12/2026	Rà soát danh mục hệ thống, tài sản số, tài khoản quản trị; kiểm tra lỗ hổng, phần mềm bảo vệ; hoàn thiện phương án ứng phó sự cố; triển khai mô hình “4 lớp” phù hợp.	PHT phụ trách CDS; CNTT	Danh mục hệ thống; biên bản rà soát; phương án ứng phó; hồ sơ khắc phục.	Hiệu trưởng
2	Hàng năm	Tuyên truyền, tập huấn nhận thức; lồng ghép giáo dục an toàn số; cử nhân sự tham gia tập huấn/diễn tập của ngành.	BGH; tổ CM; GVCN; Đoàn - Đội; CNTT	Tài liệu/chuyên đề; danh sách tham gia; minh chứng triển khai.	BGH
3	2027	Chuẩn hóa quy trình quản lý tài khoản, phân quyền, dữ liệu; rà soát yêu cầu bảo mật trong hợp đồng với nhà cung cấp hệ thống số.	CNTT; Văn phòng	Quy trình nội bộ; danh mục tài khoản; yêu cầu bảo mật trong hợp đồng.	PHT phụ trách
4	2028	Tăng cường giám sát đối với hệ thống quan trọng; tổ chức đánh giá độc lập hoặc thuê dịch vụ đánh giá khi cần; khắc phục điểm yếu phát hiện.	CNTT; đối tác kỹ thuật	Báo cáo đánh giá; kế hoạch và kết quả khắc phục.	BGH

TT	Thời gian	Nhiệm vụ trọng tâm	Đầu mối	Kết quả	Kiểm tra
5	2029	Rà soát tổng thể phương án ứng phó; tổ chức diễn tập mô phỏng; đánh giá khả năng phối hợp giữa các cơ sở/bộ phận.	CNTT; Văn phòng; BÐH	Kịch bản diễn tập; biên bản rút kinh nghiệm; phương án cập nhật.	Hiệu trưởng
6	2030	Tổng rà soát kết quả giai đoạn 2026-2030; đánh giá tồn tại, rủi ro và xây dựng định hướng giai đoạn tiếp theo.	BGH; CNTT	Báo cáo tổng kết; danh mục nhiệm vụ giai đoạn tiếp theo.	Hiệu trưởng

V. TỔ CHỨC THỰC HIỆN

1. Ban giám hiệu

- Chỉ đạo chung, chịu trách nhiệm về công tác bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong phạm vi nhà trường; quyết định các biện pháp xử lý khi có sự cố nghiêm trọng.

- Kiểm tra, đôn đốc việc thực hiện; xem xét trách nhiệm đối với trường hợp vi phạm quy định bảo mật, để xảy ra mất an toàn thông tin do chủ quan hoặc không thực hiện nhiệm vụ được giao.

- Tổ chức triển khai Kế hoạch; chỉ đạo rà soát hệ thống, tài khoản, dữ liệu, phương án ứng phó sự cố và hoạt động tuyên truyền, tập huấn có liên quan.

- Các PHT Theo dõi tiến độ, kiểm tra kết quả, tổng hợp khó khăn và tham mưu Hiệu trưởng phương án xử lý; phối hợp với Sở Giáo dục và Đào tạo, cơ quan chuyên trách và nhà cung cấp khi cần hỗ trợ kỹ thuật.

2. Ban Điều hành các cơ sở

- Tổ chức quán triệt, kiểm tra việc tuân thủ quy định bảo mật trong phạm vi phụ trách; kịp thời phản ánh nguy cơ, sự cố hoặc hành vi sử dụng dữ liệu không đúng quy định. Chỉ đạo giáo viên, nhân viên thực hiện đúng quy định về tài khoản, dữ liệu, thiết bị và nền tảng số; phối hợp triển khai nội dung giáo dục an toàn số cho học sinh.

3. Bộ phận IT

- Trực tiếp quản trị, theo dõi hạ tầng mạng, máy chủ, máy trạm, hệ thống thông tin và tài khoản quản trị được giao; thực hiện kiểm tra, cập nhật, phòng chống mã độc và xử lý cảnh báo.

- Lập, cập nhật danh mục hệ thống và tài khoản quản trị; theo dõi nhật ký, cảnh báo; thực hiện cô lập kỹ thuật ban đầu khi phát hiện dấu hiệu tấn công và báo cáo ngay Ban Giám hiệu.

- Chuẩn bị hồ sơ, minh chứng kỹ thuật; phối hợp kiểm tra, đánh giá độc lập, rà quét lỗ hổng và khắc phục theo yêu cầu.

4. Văn phòng

- Phối hợp quản lý tài khoản, hồ sơ, dữ liệu hành chính, dữ liệu học sinh và nhân sự thuộc phạm vi được phân công; bảo đảm việc khai thác, cung cấp và lưu trữ thông tin

đúng thẩm quyền.

- Phối hợp tổng hợp báo cáo định kỳ, báo cáo đột xuất; lưu trữ văn bản, biên bản, minh chứng và thông tin xử lý sự cố theo quy định.

5. Tổ chuyên môn, GVCN, GVBM

Lồng ghép nội dung an toàn, an ninh mạng và kỹ năng tự bảo vệ trên không gian mạng trong hoạt động dạy học, giáo dục phù hợp với môn học, cấp học và hướng dẫn của ngành. Giáo viên chủ nhiệm tuyên truyền, nhắc nhở học sinh bảo vệ tài khoản, dữ liệu cá nhân, nhận diện lừa đảo và báo cáo khi gặp sự cố trên môi trường số có liên quan đến hoạt động học tập, nhà trường.

6. Đoàn Thanh niên, Đội Thiếu niên

Phối hợp tổ chức tuyên truyền, chuyên đề, hoạt động trải nghiệm về ứng xử văn minh, an toàn trên không gian mạng; phát huy vai trò học sinh trong xây dựng môi trường mạng lành mạnh.

7. Toàn thể cán bộ, giáo viên, nhân viên và học sinh

Chấp hành quy định của nhà trường về sử dụng tài khoản, thiết bị, phần mềm, dữ liệu và Internet; bảo vệ thông tin cá nhân, không chia sẻ thông tin đăng nhập, không tự ý cài đặt hoặc sử dụng công cụ không được phép trên thiết bị quản trị. Khi phát hiện thư, đường dẫn, tài khoản, thiết bị hoặc hoạt động có dấu hiệu bất thường, báo ngay cho giáo viên/bộ phận phụ trách; không tự xử lý làm mất dấu vết hoặc làm sự cố lan rộng.

VI. CHẾ ĐỘ THÔNG TIN, BÁO CÁO VÀ XỬ LÝ SỰ CỐ

1. Báo cáo định kỳ

- Các bộ phận được phân công báo cáo kết quả thực hiện về Phó Hiệu trưởng phụ trách chuyển đổi số, CNTT theo yêu cầu để tổng hợp.

- Nhà trường thực hiện cập nhật kết quả triển khai, báo cáo Sở Giáo dục và Đào tạo trước ngày 15 hằng tháng theo hình thức/link báo cáo do Sở hướng dẫn; trong thời gian Kế hoạch của Sở đang áp dụng, thực hiện theo địa chỉ:

<https://forms.gle/2bXDdfTGh9gDBoAy6>.

Trường hợp Sở thay đổi hình thức báo cáo, thực hiện theo thông báo mới.

2. Báo cáo đột xuất, xử lý sự cố khẩn cấp

- Khi phát hiện sự cố nghiêm trọng như mã độc mã hóa dữ liệu tổng tiền, tấn công làm gián đoạn hệ thống, phá hoại, truy cập trái phép, rò rỉ dữ liệu cá nhân người học/nhân sự hoặc dấu hiệu lộ, lọt thông tin thuộc diện bảo vệ, bộ phận quản trị phải thực hiện ngay biện pháp cô lập kỹ thuật ban đầu và báo cáo Hiệu trưởng.

- Nhà trường thực hiện báo cáo khẩn cấp bằng văn bản hoặc phương thức điện tử nhanh nhất về Sở Giáo dục và Đào tạo (qua Văn phòng Sở) và phối hợp Công an Thành phố/cơ quan chuyên trách theo hướng dẫn trong vòng 24 giờ kể từ khi phát hiện sự cố.

- Nội dung báo cáo gồm: thời điểm phát hiện; mô tả hiện tượng/hành vi tấn công; hệ thống bị ảnh hưởng; đánh giá thiệt hại ban đầu; biện pháp cô lập đã thực hiện; nhu cầu, đề

xuất hỗ trợ.

VII. KIỂM TRA, ĐÁNH GIÁ

- Ban Giám hiệu tổ chức kiểm tra định kỳ hoặc đột xuất việc chấp hành quy định bảo mật, quản lý tài khoản, dữ liệu và thiết bị; yêu cầu khắc phục ngay các tồn tại có nguy cơ mất an toàn thông tin.

- Kết quả thực hiện được xem xét trong đánh giá mức độ hoàn thành nhiệm vụ đối với cá nhân, bộ phận được giao quản trị hệ thống, dữ liệu và triển khai công tác an ninh mạng của trường; việc xem xét phải căn cứ nhiệm vụ, trách nhiệm thực tế và quy định quản trị nội bộ của đơn vị ngoài công lập. Định kỳ cuối năm học và cuối năm, bộ phận phụ trách tham mưu sơ kết, rà soát nguy cơ, cập nhật nhiệm vụ năm tiếp theo; năm 2030 tổ chức tổng kết giai đoạn 2026-2030.

Trên đây là Kế hoạch triển khai thực hiện bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu giai đoạn 2026-2030 của Trường Trung - Tiểu học Pétrus Ký. Các bộ phận, cá nhân được phân công căn cứ chức năng, nhiệm vụ tổ chức thực hiện nghiêm túc; trường hợp phát sinh khó khăn, vướng mắc báo cáo Ban Giám hiệu để xem xét, xử lý hoặc đề nghị cơ quan có thẩm quyền hướng dẫn./.

Nơi nhận:

- Sở Giáo dục và Đào tạo TP.HCM (báo cáo);
- Hội đồng trường (để biết);
- BGH, BDH các cấp học/cơ sở;
- Văn phòng, CNTT, Kế toán;
- Các tổ chuyên môn, GVCN, Đoàn - Đội;
- Lưu: VT.

HIỆU TRƯỞNG



Phạm Ngọc Nam