UBND TỈNH LÂM ĐỒNG **SỞ GIÁO DỤC VÀ ĐÀO TẠO**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 76 /KH-SGDĐT	*Lâm Đồng, ngày 24 tháng 3 năm 2026*

KẾ HOẠCH
Triển khai thực hiện công tác bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu trong ngành Giáo dục và Đào tạo

Thực hiện Kế hoạch số 1743/KH-UBND ngày 04/02/2026 của UBND tỉnh Lâm Đồng triển khai thực hiện Thông báo Kết luận số 06-TB/CQTTBCĐ, ngày 27/9/2025 của Đồng chí Tổng Bí thư Tô Lâm về công tác bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu trên địa bàn tỉnh Lâm Đồng (Kế hoạch số 1743/KH-UBND); Sở Giáo dục và Đào tạo ban hành Kế hoạch triển khai thực hiện với các nội dung cụ thể như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Quán triệt, thực hiện nghiêm túc, quyết liệt các nhiệm vụ bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu theo Thông báo Kết luận số 06-TB/CQTTBCĐ ngày 27/9/2025 của Cơ quan Thường trực Ban Chỉ đạo Trung ương về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số tại Phiên họp Thường trực Ban Chỉ đạo về công tác bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu (Kết luận số 06-TB/CQTTBCĐ); Công văn số 1406/TTg-KSTT ngày 30/10/2025 của Thủ tướng Chính phủ về việc triển khai công tác bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu (Công văn số 1406/TTg-KSTT); Công văn số 05-CV/BCĐ ngày 27/11/2025 của Ban Chỉ đạo tỉnh về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số về việc triển khai thực hiện Thông báo Kết luận số 06-TB/CQTTBCĐ ngày 27/9/2025 của Cơ quan Thường trực Ban Chỉ đạo Trung ương (Công văn số 05-CV/BCĐ) và Kế hoạch số 1743/KH-UBND. Xác định rõ việc bảo đảm an ninh mạng và an toàn dữ liệu là điều kiện tiên quyết để chuyển đổi số thành công trong ngành giáo dục, cũng như phục vụ cải cách hành chính và nâng cao hiệu quả quản lý nhà nước.

- Tạo ra sự chuyển biến thực chất về nhận thức và trách nhiệm của người đứng đầu các cơ sở giáo dục, cùng toàn thể cán bộ, công chức, viên chức, giáo viên, nhân viên và học sinh trong toàn ngành. Đưa kết quả thực hiện công tác bảo đảm an ninh mạng, an toàn dữ liệu trở thành tiêu chí, chỉ tiêu thi đua và là căn cứ để đánh giá mức độ hoàn thành nhiệm vụ của các cơ quan, đơn vị trực thuộc.

- Bảo đảm an toàn tuyệt đối cho các hệ thống thông tin trọng yếu của Sở Giáo dục và Đào tạo và các đơn vị trực thuộc Sở (bao gồm hệ thống cơ sở dữ liệu (CSDL) ngành, hệ thống quản lý thi và tuyển sinh, cổng thông tin điện tử, thư điện tử công vụ và các phần mềm điều hành giáo dục khác).

- Chủ động phòng ngừa từ sớm, từ xa; nâng cao năng lực giám sát, phát hiện sớm, cảnh báo, ứng cứu và xử lý kịp thời các sự cố mất an toàn thông tin. Giảm thiểu tối đa thiệt hại, bảo đảm các hoạt động quản lý, công tác dạy và học của ngành giáo dục luôn diễn ra ổn định, thông suốt và không bị gián đoạn.

2. Yêu cầu

- Việc triển khai phải đồng bộ, có sự phân công rõ trách nhiệm của cơ quan, đơn vị liên quan, có thời hạn hoàn thành và sản phẩm đầu ra cụ thể. Tuân thủ tuyệt đối nguyên tắc "rõ người, rõ việc, rõ tiến độ, rõ kết quả, rõ trách nhiệm" đối với từng phòng chuyên môn, nghiệp vụ, đơn vị trực thuộc Sở và các cơ sở giáo dục.

- Thực hiện nghiêm nguyên tắc "an toàn, an ninh mạng ngay từ khâu thiết kế" đối với các dự án, phần mềm mới; ưu tiên bảo vệ các hệ thống thông tin quan trọng và CSDL trọng yếu của ngành giáo dục. Kiên quyết khắc phục dứt điểm tình trạng "nợ tuân thủ" trong các hệ thống thông tin do cơ sở giáo dục quản lý.

- Yêu cầu các hệ thống thông tin phải được đánh giá hiện trạng và khả năng bảo đảm an toàn thông tin mạng định kỳ. Phải chuyển hoạt động ứng phó sự cố từ bị động sang chủ động, đặc biệt chú trọng việc chủ động thực hiện giám sát và rà quét lỗ hổng định kỳ trên các hệ thống thông tin thuộc phạm vi quản lý.

- Việc kết nối, chia sẻ dữ liệu ngành phải được thực hiện trên nguyên tắc bảo mật, an toàn, đúng pháp luật. Cơ quan, đơn vị, các cơ sở giáo dục phải thực hiện theo đúng quy trình điều phối, ứng cứu sự cố của tỉnh và đảm bảo công tác thông tin, báo cáo đúng biểu mẫu, thời hạn quy định.

II. NHIỆM VỤ VÀ GIẢI PHÁP TRỌNG TÂM

1. Tuyên truyền, phổ biến quán triệt, nâng cao nhận thức và trách nhiệm trong công tác bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu

a) Nội dung thực hiện:

- Tổ chức quán triệt sâu rộng nội dung Thông báo Kết luận số 06-TB/CQTTBCĐ, Công văn số 05-CV/BCĐ, Công văn số 1406/TTg-KSTT và Kế hoạch số 1743/KH-UBND đến toàn thể cán bộ, công chức, viên chức, người lao động trong cơ quan quản lý và các cơ sở giáo dục.

- Đẩy mạnh tuyên truyền, phổ biến các văn bản quy phạm pháp luật (Luật An ninh mạng, Luật Bảo vệ bí mật nhà nước, Luật Bảo vệ dữ liệu cá nhân, Luật Dữ liệu) và các tài liệu hướng dẫn chuyên môn về an toàn thông tin mạng đồng bộ, có chiều sâu, đa dạng về nội dung và hình thức trên Cổng thông tin điện tử và các phương tiện thông tin đại chúng.

- Hướng dẫn kỹ năng sử dụng không gian mạng an toàn cho cán bộ, giáo viên, nhân viên và học sinh; triển khai thực hiện hiệu quả mô hình “Bình dân học vụ số” nhằm phổ cập kỹ năng an toàn số.

- Đưa kết quả thực hiện công tác bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu vào tiêu chí đánh giá, xếp loại thi đua hằng năm đối với các tập thể và cá

nhân theo hướng dẫn của cấp có thẩm quyền. Chú trọng đặc biệt đến trách nhiệm của người đứng đầu cơ quan, đơn vị, trường học.

- Tổ chức kiểm tra nội bộ việc chấp hành và tuân thủ các quy định về an ninh mạng, bảo mật thông tin, an toàn dữ liệu tại các cơ quan, đơn vị.

b) Đơn vị chủ trì thực hiện/tham mưu:

- Thủ trưởng các cơ sở giáo dục, trung tâm Giáo dục nghề nghiệp - Giáo dục thường xuyên, Trưởng các phòng chuyên môn, nghiệp vụ chủ trì triển khai tại đơn vị mình.

- Văn phòng Sở làm đầu mối đôn đốc, theo dõi. Tổ chức kiểm tra nội bộ việc chấp hành và tuân thủ các quy định về an ninh mạng, bảo mật thông tin, an toàn dữ liệu tại cơ quan Sở.

- Phòng Tổ chức cán bộ tham mưu lồng ghép nội dung bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu vào tiêu chí đánh giá, xếp loại thi đua hằng năm khi có hướng dẫn của cấp có thẩm quyền.

c) Thời gian thực hiện: Thực hiện thường xuyên, liên tục hằng năm.

2. Giáo dục an ninh mạng, bảo mật thông tin, an toàn dữ liệu trong chương trình học

a) Nội dung thực hiện:

Tổ chức nghiên cứu, cập nhật các nội dung kiến thức, kỹ năng cơ bản về an ninh mạng, bảo mật thông tin, an toàn dữ liệu, cũng như văn hóa ứng xử trên không gian mạng vào chương trình giáo dục. Triển khai bắt buộc đối với các cấp học từ trung học cơ sở (THCS) trở lên, giúp thế hệ trẻ có ý thức từ sớm về việc sử dụng không gian mạng an toàn.

b) Đơn vị chủ trì thực hiện/tham mưu:

- Phòng Giáo dục Trung học chủ trì tham mưu, quản lý việc thực hiện chương trình, nội dung, kế hoạch dạy học và hướng dẫn các cơ sở giáo dục trung học triển khai.

c) Thời gian thực hiện: Duy trì thực hiện thường xuyên hằng năm.

3. Rà soát, hoàn thiện các quy chế, quy định về an ninh mạng, bảo mật thông tin, an toàn dữ liệu trong ngành giáo dục

a) Nội dung thực hiện:

- Tập trung xây dựng, rà soát và hoàn thiện quy định, quy chế sử dụng mạng máy tính nội bộ, mạng máy tính có kết nối Internet trong các cơ quan nhà nước và trường học. Đảm bảo các quy định này đồng bộ với quy định của Trung ương về quản lý và bảo vệ bí mật nhà nước trên không gian mạng.

- Hoàn thành việc xác định cấp độ và triển khai phương án bảo đảm an toàn theo cấp độ đối với 100% hệ thống thông tin do các cơ sở giáo dục làm chủ quản.

- Thực hiện kiểm tra, khắc phục những lỗ hổng bảo mật, khắc phục tình trạng "nợ tuân thủ" các điều kiện về an ninh, an toàn mạng.

b) Đơn vị chủ trì thực hiện/tham mưu:

- Văn phòng Sở chủ trì, phối hợp với các phòng chuyên môn, nghiệp vụ tham mưu hoàn thiện hệ thống văn bản, quy chế liên quan đến an toàn thông tin của Sở (bao gồm quy chế sử dụng mạng máy tính nội bộ, mạng máy tính có kết nối Internet trong các cơ quan nhà nước và trường học).

- Thủ trưởng các cơ sở giáo dục triển khai thực hiện xác định cấp độ, triển khai các phương án đảm bảo an toàn theo cấp độ và khắc phục lỗ hổng bảo mật đối với các phần mềm, hệ thống thuộc đơn vị mình theo hướng dẫn của cơ quan chức năng.

c) Thời gian thực hiện:

- Việc xây dựng, hoàn thiện quy định, quy chế sử dụng mạng nội bộ, mạng máy tính: Hoàn thành trước ngày 15/4/2026.

- Việc xác định cấp độ an toàn và khắc phục "nợ tuân thủ": Thực hiện theo hướng dẫn của cấp có thẩm quyền, hoàn thành trước ngày 31/12/2026.

4. Ứng phó sự cố, bảo vệ và chuẩn hóa dữ liệu

a) Nội dung thực hiện:

- Thực hiện ứng phó sự cố, bảo đảm an toàn thông tin mạng theo hướng dẫn tại Kế hoạch số 42/KH-SGDĐT ngày 26/02/2026 của Sở Giáo dục và Đào tạo về ứng phó sự cố, bảo đảm an toàn thông tin mạng trong lĩnh vực Giáo dục và Đào tạo. Chuyển hoạt động ứng phó sự cố từ bị động sang chủ động thông qua việc thường xuyên giám sát và rà quét lỗ hổng định kỳ trên các hệ thống thông tin thuộc phạm vi quản lý.

- Khi xảy ra sự cố, phải tuân thủ nghiêm ngặt quy trình xử lý khẩn cấp ban đầu: Cách ly ngay hệ thống/máy trạm bị nhiễm khỏi mạng; nhanh chóng sao lưu dữ liệu quan trọng; tạm dừng các dịch vụ nếu cần thiết. Tuyệt đối không tự ý xử lý nếu vượt thẩm quyền. Phải thực hiện báo cáo ngay lập tức (báo cáo ban đầu, báo cáo diễn biến) để phối hợp ứng cứu.

- Thực hiện chuẩn hóa, làm sạch dữ liệu; thiết lập cơ chế kết nối, chia sẻ, liên thông dữ liệu an toàn với CSDL quốc gia (như CSDL quốc gia về dân cư) và Trung tâm dữ liệu quốc gia, kiên quyết khắc phục tình trạng cát cứ, phân mảnh dữ liệu. Các đơn vị phải chịu trách nhiệm trực tiếp về tính chính xác, đầy đủ, kịp thời của dữ liệu do mình quản lý.

- Đảm bảo nguyên tắc "an toàn, an ninh mạng ngay từ khâu thiết kế" đối với việc xây dựng mới các phần mềm, CSDL trọng yếu.

b) Đơn vị chủ trì thực hiện/tham mưu:

- Văn phòng Sở: Làm đầu mối chủ trì, tiếp nhận thông báo sự cố của toàn ngành và trực tiếp điều phối, liên hệ phối hợp với Công an tỉnh (Đội Ứng cứu sự cố tỉnh), Trung tâm Hạ tầng và Công nghệ số, các doanh nghiệp cung cấp dịch vụ

công nghệ thông tin (CNTT), viễn thông để xử lý. Chỉ đạo việc giám sát, sao lưu dữ liệu định kỳ và rà quét lỗ hổng bảo mật đối với các hệ thống cấp Sở.

- Thủ trưởng các đơn vị trực thuộc, các trường học: Chịu trách nhiệm chính tại đơn vị mình. Cử cán bộ phụ trách CNTT kiêm nhiệm an toàn thông tin mạng; thực hiện cài đặt phần mềm diệt virus bản quyền, thay đổi mật khẩu thường xuyên, sao lưu dữ liệu giáo viên/học sinh định kỳ và báo cáo khẩn cấp ngay khi phát hiện dấu hiệu bất thường.

c) Thời gian thực hiện:

- Xây dựng phương án ứng phó sự cố, khôi phục dữ liệu tại các đơn vị: Hoàn thành trong Quý II/2026.

- Công tác chuẩn hóa, làm sạch và bảo đảm điều kiện kết nối dữ liệu: Hoàn thành trước ngày 31/12/2026.

5. Bảo đảm nguồn lực tài chính và phát triển nhân lực

a) Nội dung thực hiện:

- Ưu tiên bố trí ngân sách nhà nước hằng năm cho công tác bảo đảm an ninh mạng, bảo mật thông tin và an toàn dữ liệu. Thực hiện nghiêm quy định bảo đảm an ninh mạng là thành phần bắt buộc trong mọi dự án CNTT, yêu cầu tỷ lệ kinh phí chi cho các sản phẩm, dịch vụ an ninh mạng, an toàn dữ liệu đạt tối thiểu 15% tổng kinh phí triển khai dự án. Các đơn vị chủ động cân đối ngân sách để mua sắm, nâng cấp, gia hạn bản quyền trang thiết bị, phần mềm bảo mật, công cụ phục vụ ứng phó và khắc phục sự cố.

- Phân công rõ cán bộ, công chức, viên chức phụ trách chuyên trách hoặc kiêm nhiệm quản lý an toàn thông tin mạng. Tạo điều kiện và cử cán bộ tham gia các khóa đào tạo, bồi dưỡng, tập huấn chuyên sâu, diễn tập thực chiến về phòng, chống tấn công mạng, ứng cứu sự cố do tỉnh hoặc các cơ quan chuyên trách tổ chức để nâng cao năng lực.

b) Đơn vị chủ trì thực hiện/tham mưu:

- Phòng Kế hoạch - Tài chính: Chủ trì tham mưu bố trí kinh phí và kiểm soát yêu cầu tỷ lệ 15% ngân sách cho an ninh mạng, bảo mật thông tin, an toàn dữ liệu trong các dự án CNTT do Sở làm chủ đầu tư.

- Phòng Tổ chức cán bộ: Phối hợp rà soát, đánh giá đội ngũ cán bộ phụ trách CNTT và tham mưu xây dựng kế hoạch đào tạo, bồi dưỡng nhân lực an toàn thông tin cho toàn ngành.

- Thủ trưởng các cơ sở giáo dục/đơn vị trực thuộc: Phân công cán bộ phụ trách CNTT kiêm nhiệm an toàn thông tin tại đơn vị; cân đối ngân sách để mua sắm, trang bị phần mềm, phần cứng bảo mật (phần mềm diệt virus bản quyền...).

c) Thời gian thực hiện: Thực hiện thường xuyên.

III. TỔ CHỨC THỰC HIỆN

1. Văn phòng Sở, các phòng chuyên môn, nghiệp vụ thuộc Sở

- Văn phòng Sở: Tham mưu hoàn thiện hệ thống văn bản, quy chế liên quan đến an toàn thông tin của Sở, đầu mối đôn đốc, theo dõi, điều phối xử lý sự cố về an toàn, an ninh mạng và tổng hợp báo cáo định kỳ.

- Phòng Giáo dục Trung học: Chủ trì tham mưu, hướng dẫn cập nhật kiến thức, kỹ năng an ninh mạng, bảo mật thông tin, an toàn dữ liệu vào chương trình giảng dạy và đẩy mạnh ứng dụng CNTT, chuyển đổi số trong cơ sở giáo dục. Phối hợp với Văn phòng Sở theo dõi, đôn đốc việc thực hiện an toàn thông tin gắn với các hoạt động chuyên môn của cấp học.

- Phòng Kế hoạch - Tài chính: Chủ trì thẩm định các thiết bị, phần mềm CNTT; tham mưu bố trí ngân sách, đảm bảo tỷ lệ tối thiểu 15% kinh phí cho an ninh mạng, bảo mật thông tin, an toàn dữ liệu trong các dự án CNTT.

- Phòng Tổ chức cán bộ: Tham mưu lồng ghép tiêu chí an ninh mạng, bảo mật thông tin, an toàn dữ liệu vào đánh giá thi đua, khen thưởng theo hướng dẫn của cấp có thẩm quyền; tổ chức bồi dưỡng, nâng cao năng lực cho đội ngũ cán bộ phụ trách CNTT.

- Các phòng chuyên môn, nghiệp vụ khác thuộc Sở: Phối hợp triển khai thực hiện, kiểm tra việc tuân thủ quy định an toàn thông tin, bảo mật dữ liệu, ứng dụng CNTT theo từng cấp học và lĩnh vực quản lý phụ trách.

2. Các cơ sở giáo dục trực thuộc Sở

- Xây dựng kế hoạch cụ thể tại đơn vị; cử cán bộ làm đầu mối phụ trách an toàn thông tin.

- Tổ chức triển khai hiệu quả việc giảng dạy các nội dung về an ninh mạng, bảo mật thông tin, an toàn dữ liệu trong chương trình học và lồng ghép vào các hoạt động giáo dục khác (đối với các trường từ THCS trở lên).

- Báo cáo ngay mọi sự cố an toàn thông tin mạng (nếu có) về Sở Giáo dục và Đào tạo (qua Văn phòng Sở).

3. Ủy ban nhân dân các xã, phường, đặc khu

Phối hợp với Sở Giáo dục và Đào tạo trong tổ chức quán triệt và triển khai thực hiện các nội dung của Kế hoạch này đến các cơ sở giáo dục trên địa bàn quản lý.

IV. CHẾ ĐỘ BÁO CÁO

Định kỳ hằng năm (trước ngày 05/11 hoặc đột xuất khi có yêu cầu của cấp có thẩm quyền), Ủy ban nhân dân các xã, phường, đặc khu và các đơn vị trực thuộc Sở báo cáo tình hình và kết quả thực hiện về Sở Giáo dục và Đào tạo để tổng hợp, báo cáo các cơ quan cấp trên theo quy định.

Trên đây là Kế hoạch triển khai thực hiện công tác bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu trong ngành Giáo dục và Đào tạo. Sở Giáo dục và Đào

tạo đề nghị lãnh đạo các phòng chuyên môn, nghiệp vụ, các đơn vị trực thuộc Sở căn cứ chức năng, nhiệm vụ được giao xây dựng kế hoạch cụ thể và nghiêm túc tổ chức triển khai thực hiện. Trong quá trình thực hiện, nếu có khó khăn, vướng mắc phát sinh, các cơ quan, đơn vị kịp thời phản ánh về Sở Giáo dục và Đào tạo (qua Phòng Giáo dục Trung học) để được hướng dẫn hoặc trình Lãnh đạo Sở xem xét, quyết định./.

Nơi nhận:
- Giám đốc, các PGĐ Sở GDĐT;
- UBND xã, phường, đặc khu (phối hợp);
- Văn phòng Sở;
- Các phòng CM, NV thuộc Sở;
- Các cơ sở giáo dục trực thuộc Sở GDĐT (thực hiện);
- Lưu: VT, GDTrH

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ GIÁO DỤC VÀ ĐÀO TẠO
TỈNH LÂM ĐỒNG

Phan Thanh Hải