

Số: /KH-SGDĐT

Bình Phước, ngày tháng 5 năm 2023

KẾ HOẠCH

Triển khai thực hiện Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030 ngành Giáo dục và Đào tạo tỉnh Bình Phước

Thực hiện Kế hoạch số 151/KH-UBND ngày 08/5/2023 của UBND tỉnh về triển khai thực hiện Quyết định số 964/QĐ-TTg ngày 10/8/2022 của Thủ tướng Chính phủ về phê duyệt Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030, Sở Giáo dục và Đào tạo (GD&ĐT) xây dựng Kế hoạch triển khai thực hiện như sau:

I. MỤC ĐÍCH, YÊU CẦU

Bảo đảm sự lãnh đạo toàn diện của Đảng và quản lý của Nhà nước trong công tác bảo đảm an toàn, an ninh mạng nhằm chủ động phòng ngừa, sẵn sàng ứng phó với các thách thức từ không gian mạng trong thời đại Cách mạng công nghiệp lần thứ tư, nhất là trong bối cảnh cả nước đang đẩy mạnh quá trình chuyển đổi số. Tổ chức triển khai thực hiện nghiêm túc, hiệu quả các nhiệm vụ được giao tại Quyết định số 964/QĐ-TTg ngày 10/8/2022 của Thủ tướng Chính phủ.

Phát huy sức mạnh của hệ thống chính trị và toàn xã hội, nhất là mối quan hệ giữa Nhà nước, doanh nghiệp, các trường học và người dân trong công tác bảo đảm an toàn, an ninh mạng. Chuyển đổi căn bản về nhận thức, cách làm và xây dựng, phát triển lực lượng bảo đảm an toàn, an ninh mạng hiện đại, chuyên nghiệp, đáp ứng yêu cầu thực tiễn.

Xác định các nội dung, nhiệm vụ trọng tâm và giải pháp thực hiện nhằm đảm bảo tập trung, xuyên suốt, đồng bộ và thống nhất. Phối hợp chặt chẽ với các sở, ban, ngành liên quan trong quá trình thực hiện nhằm hoàn thành tốt các nhiệm vụ được giao, bảo đảm an toàn, an ninh mạng trong phạm vi quản lý.

II. MỤC TIÊU

1. Mục tiêu tổng quát: Xây dựng không gian mạng phát triển văn minh, lành mạnh, là động lực tham gia cuộc Cách mạng công nghiệp lần thứ tư. Nâng lực về bảo đảm an toàn, an ninh mạng được nâng cao, chủ động, sẵn sàng ứng phó với các nguy cơ, thách thức từ không gian mạng nhằm bảo vệ vững chắc chủ quyền, lợi ích và đảm bảo quốc phòng, an ninh và trật tự an toàn trong trường học; bảo vệ chủ quyền quốc gia trên không gian mạng và công cuộc chuyển đổi số và quyền, lợi ích hợp pháp của các tổ chức, cá nhân trên không gian mạng.

2. Mục tiêu cụ thể

2.1. Mục tiêu cụ thể đến năm 2025

Nâng cao năng lực, thứ hạng về an toàn, an ninh mạng của ngành giáo dục.

Xây dựng hệ thống thể trận An ninh nhân dân trên không gian mạng có khả năng kết nối, chia sẻ thông tin, tiếp nhận và xử lý các thông tin gây hại tới không gian mạng trên địa bàn tỉnh.

Từng bước hình thành lực lượng bảo đảm an toàn, an ninh mạng tại cơ quan Sở GD&ĐT, các đơn vị trường học; đảm bảo mỗi trường học có một bộ phận được giao nhiệm vụ làm đầu mối, chịu trách nhiệm về công tác bảo đảm an toàn, an ninh mạng. Khuyến khích các trường học thành lập một Tổ bảo đảm an toàn, an ninh mạng của đơn vị.

Các đơn vị trường học thực hiện công tác bảo đảm an toàn, an ninh mạng theo quy định của pháp luật về an toàn thông tin và an ninh mạng.

Bảo vệ cơ sở hạ tầng không gian mạng và các hệ thống thông tin quan trọng của các cơ quan Đảng và Nhà nước trên địa bàn tỉnh.

Triển khai các hoạt động nhằm nâng cao nhận thức, kỹ năng bảo đảm an toàn, an ninh mạng tiếp cận đông đảo tới người dùng Internet trong các đơn vị trường học.

Phấn đấu 80% cán bộ quản lý, giáo viên, nhân viên ngành giáo dục có cơ hội tiếp cận các hoạt động nâng cao nhận thức, kỹ năng và công cụ bảo đảm an toàn, an ninh mạng.

Áp dụng chính sách phù hợp cho thúc đẩy khởi nghiệp về an toàn, an ninh mạng góp phần xây dựng nền móng hình thành nên công nghiệp an ninh mạng và công nghiệp an toàn thông tin mạng.

Kinh phí phục vụ bảo đảm an toàn, an ninh mạng đạt tối thiểu 10% kinh phí chi cho khoa học công nghệ, chuyển đổi số và ứng dụng công nghệ thông tin.

2.2. Mục tiêu cụ thể đến năm 2030

Duy trì và nâng cao năng lực, thứ hạng về an toàn, an ninh mạng của các đơn vị trường học trong tỉnh, góp phần nâng cao thứ hạng của tỉnh trên bảng xếp hạng toàn quốc.

Xây dựng thể trận An ninh nhân dân trên không gian mạng với sự tham gia tích cực, đông đảo của cán bộ quản lý, giáo viên, nhân viên, quần chúng Nhân dân trên địa bàn tỉnh.

Củng cố, tăng cường lực lượng bảo đảm an toàn, an ninh mạng.

Phấn đấu 90% cán bộ quản lý, giáo viên, nhân viên ngành giáo dục có cơ hội tiếp cận các hoạt động nâng cao nhận thức, kỹ năng và công cụ bảo đảm an toàn, an ninh mạng.

III. NHIỆM VỤ, GIẢI PHÁP

1. Nhiệm vụ chung

Tăng cường các hoạt động bảo đảm an toàn, an ninh mạng trong phạm vi quản lý; tuân thủ tiêu chuẩn, quy chuẩn kỹ thuật, hướng dẫn nghiệp vụ của Bộ Công an, Bộ Thông tin và Truyền thông và các quy định liên quan; ưu tiên sử dụng các sản phẩm, giải pháp, dịch vụ an toàn thông tin mạng của Việt Nam sản xuất, chế tạo (Make in Viet Nam) và an ninh mạng tự chủ. Gắn kết công tác bảo đảm an toàn, an ninh mạng với công tác triển khai chuyển đổi số,

ứng dụng công nghệ thông tin, phát triển Chính phủ điện tử hướng tới Chính phủ số và phát triển đô thị thông minh, kinh tế số, xã hội số.

Chủ động rà soát, phát hiện và xử lý hoặc phối hợp với cơ quan chức năng có thẩm quyền xử lý các thông tin vi phạm pháp luật trên môi trường mạng thuộc phạm vi quản lý; tăng cường hoạt động kiểm tra, công bố và xử lý nghiêm các hành vi vi phạm theo quy định.

Chuyển đổi căn bản về nhận thức và cách làm để thích ứng một cách chủ động, linh hoạt và giảm thiểu các nguy cơ, đe dọa an toàn, an ninh mạng (cyber resilience): Từ mô hình bảo vệ phân tán sang mô hình bảo vệ tập trung, từ bị động ứng cứu sự cố sang chủ động dự báo sớm, cảnh báo sớm, phòng ngừa và ứng phó hiệu quả; từ đơn độc bảo vệ, giấu kín thông tin bị tấn công mạng sang chủ động hợp tác, chia sẻ thông tin nhằm chủ động phòng ngừa và hỗ trợ xử lý sự cố, phục hồi hoạt động bình thường của hệ thống thông tin.

Chỉ đạo các đơn vị trường học kiểm tra, rà soát, đánh giá và có biện pháp tăng cường bảo đảm an toàn, an ninh mạng đối với các hệ thống hạ tầng thông tin, hệ thống cơ sở dữ liệu và các hệ thống thông tin quan trọng khác đang quản lý, vận hành, khai thác.

Ưu tiên bố trí nguồn lực và các điều kiện cần thiết để triển khai công tác bảo đảm an toàn, an ninh mạng trong hoạt động nội bộ của cơ quan, các đơn vị trường học.

Kiểm tra, đánh giá và báo cáo kết quả triển khai thực hiện ở các cơ quan, đơn vị trường học định kỳ hàng năm hoặc đột xuất theo yêu cầu của cơ quan có thẩm quyền.

2. Nhiệm vụ cụ thể

2.1. Tăng cường vai trò lãnh đạo của Đảng và quản lý của Nhà nước

Công tác bảo đảm an toàn, an ninh mạng phải đặt dưới sự lãnh đạo toàn diện của Đảng, sự quản lý chặt chẽ của Nhà nước và sự vào cuộc của cả hệ thống chính trị; trong đó, Tiểu ban An toàn, An ninh mạng tỉnh điều phối chung, chủ động phối hợp với các sở, ban, ngành liên quan thực hiện theo chức năng, nhiệm vụ được giao.

Thường xuyên phổ biến, quán triệt các chủ trương của Đảng và chính sách, pháp luật của Nhà nước về an toàn, an ninh mạng; xác định an toàn, an ninh mạng là trọng tâm của quá trình chuyển đổi số, là nhiệm vụ trọng yếu, thường xuyên và lâu dài.

Nâng cao nhận thức, trách nhiệm của cán bộ quản lý, giáo viên, nhân viên, học sinh và cha mẹ học sinh trong công tác bảo đảm an toàn, an ninh mạng. Hiệu trưởng trực tiếp lãnh đạo, chỉ đạo và chịu trách nhiệm về công tác an toàn, an ninh mạng; chủ động rà soát, xác định rõ những vấn đề trọng tâm, trọng điểm để chỉ đạo triển khai thực hiện đảm bảo hiệu quả.

Vận động cán bộ quản lý, giáo viên, nhân viên và học sinh tích cực tham gia hiệu quả trong công tác bảo đảm an toàn, an ninh mạng và chủ động ứng phó với các nguy cơ, thách thức từ không gian mạng.

Ưu tiên chuyển giao và ứng dụng mạnh mẽ công nghệ, kỹ thuật an toàn, an ninh mạng; thúc đẩy nghiên cứu, tạo môi trường thuận lợi để các tổ chức, cá nhân tham gia xây dựng công nghiệp an toàn thông tin mạng và công nghiệp an ninh mạng. Tăng cường hợp tác giữa

các cơ quan nhà nước với các doanh nghiệp trong thực thi các chính sách về an toàn, an ninh mạng. Đẩy mạnh phổ biến kỹ năng tham gia không gian mạng an toàn.

2.2. Nghiên cứu, rà soát và đề xuất cấp có thẩm quyền xem xét sửa đổi, bổ sung các văn bản quy phạm pháp luật về an ninh mạng, về điều kiện kinh doanh các sản phẩm, dịch vụ an ninh mạng, nhất là các sản phẩm, dịch vụ sử dụng trong hệ thống thông tin quan trọng về an ninh quốc gia, hệ thống thông tin của cơ quan nhà nước; về bảo đảm an toàn thông tin mạng cho giao dịch điện tử, chuyển đổi số, hạ tầng số, nền tảng số, dữ liệu số, bảo vệ thông tin cá nhân trên mạng.

2.3. Bảo vệ hạ tầng số, nền tảng số, dữ liệu số và cơ sở hạ tầng không gian mạng

Bảo đảm an toàn, an ninh mạng trong quá trình triển khai thực hiện Chính phủ điện tử, chuyển đổi số. Xác định cấp độ an toàn thông tin và triển khai phương án đảm bảo an toàn hệ thống thông tin theo cấp độ đối với các nền tảng số, cơ sở dữ liệu quan trọng; ưu tiên sử dụng sản phẩm an toàn, an ninh mạng do Việt Nam sản xuất.

Chủ động giám sát, phát hiện và công bố các hành vi vi phạm quy định pháp luật thuộc phạm vi quản lý trên các nền tảng số. Xử lý theo thẩm quyền hoặc phối hợp với đơn vị chức năng xử lý các tổ chức, cá nhân vi phạm, gỡ bỏ thông tin vi phạm trên các nền tảng số.

2.4. Bảo vệ hệ thống thông tin của các cơ quan Đảng, Nhà nước

Nâng cao trách nhiệm, ý thức tự bảo vệ hệ thống thông tin thuộc phạm vi cơ quan, đơn vị quản lý. Gắn trách nhiệm của người đứng đầu cơ quan, đơn vị chủ quản hệ thống thông tin với trách nhiệm bảo đảm an toàn, an ninh mạng.

Xây dựng, cập nhật và vận hành hệ thống thông tin theo tiêu chuẩn, quy chuẩn kỹ thuật về an toàn, an ninh mạng.

Rà soát, lập hồ sơ đề nghị đưa các hệ thống thông tin trọng yếu, phù hợp với quy định của pháp luật vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

Thực hiện nghiêm túc các quy định pháp luật về bảo vệ an ninh mạng; xác định cấp độ và trách nhiệm bảo đảm an toàn hệ thống thông tin theo từng cấp độ và triển khai mô hình bảo vệ 4 lớp trước khi đưa vào sử dụng.

Chủ động giám sát, kịp thời phát hiện nguy cơ mất an toàn, an ninh mạng trong quá trình thi công, lắp đặt thiết bị trong các hệ thống thông tin. Ưu tiên sử dụng sản phẩm, giải pháp an toàn, an ninh mạng do Việt Nam sản xuất.

Tăng cường nguồn lực, thường xuyên nâng cấp hệ thống, cập nhật bản quyền, nâng cao nhận thức và kỹ năng về an toàn, an ninh mạng cho cán bộ, công chức, viên chức và người lao động. Tối thiểu 1 năm/ 1 lần tham gia diễn tập, hướng dẫn, kiểm tra, ứng phó và ứng cứu sự cố an toàn, an ninh mạng do tỉnh tổ chức.

Phối hợp với đơn vị chuyên trách về an ninh mạng của tỉnh kết nối với Trung tâm An ninh mạng quốc gia để giám sát an ninh mạng.

2.5. Tạo lập niềm tin số, xây dựng môi trường mạng trung thực, văn minh, lành mạnh và phòng, chống vi phạm pháp luật trên không gian mạng

Tổ chức tiếp nhận, xử lý thông tin về tội phạm trên không gian mạng để quần chúng nhân dân phản ánh kịp thời, trực tiếp đối với các hành vi vi phạm pháp luật trên không gian mạng.

Giám sát, phát hiện và phối hợp với cơ quan chức năng và các doanh nghiệp nền tảng số xử lý tin giả, thông tin vi phạm pháp luật trong phạm vi quản lý.

Đẩy mạnh xây dựng phong trào toàn dân bảo vệ an ninh Tổ quốc trên không gian mạng phù hợp với thực tiễn chuyển đổi số.

Duy trì các website, trang mạng xã hội, tài khoản trên môi trường mạng uy tín, dễ tương tác để tuyên truyền, định hướng thông tin, dư luận và phản bác hiệu quả các thông tin tiêu cực về đất nước, con người Việt Nam.

2.6. Đào tạo và phát triển nguồn nhân lực

Ưu tiên bố trí nguồn lực và điều kiện cần thiết để triển khai công tác bảo đảm an toàn, an ninh mạng trong hoạt động nội bộ của cơ quan, đơn vị.

Triển khai hiệu quả Đề án “Đào tạo và phát triển nguồn nhân lực an toàn thông tin giai đoạn 2021 - 2025”; phát triển đội ngũ chuyên gia xuất sắc về an toàn thông tin mạng của tỉnh và xây dựng đội ngũ cán bộ làm công tác an ninh, an toàn thông tin mạng các cơ quan, tổ chức, doanh nghiệp có chất lượng. Tuyên dương, khen thưởng kịp thời đối với các cơ quan, tổ chức, doanh nghiệp và cá nhân có cống hiến cho sự nghiệp bảo vệ an toàn, an ninh mạng.

Kịp thời khen thưởng đối với các tổ chức, cá nhân có thành tích xuất sắc trong công tác bảo đảm an toàn, an ninh mạng.

2.7. Tuyên truyền, phổ biến, nâng cao nhận thức và kỹ năng đảm bảo an toàn, an ninh mạng

Tăng cường công tác tuyên truyền, nâng cao nhận thức và phổ biến kiến thức, trang bị kỹ năng bảo đảm an toàn thông tin tới toàn thể người sử dụng Internet; triển khai các hoạt động nhằm trang bị kỹ năng cho các nhóm người yếu thế, dễ bị tổn thương trong xã hội.

Cung cấp kịp thời các thông tin chính thống để người dân nắm bắt, cùng phản biện tin giả, thông tin sai sự thật, vi phạm pháp luật trên môi trường mạng.

Tuyên truyền, phổ biến về thói quen, trách nhiệm, kỹ năng an toàn, an ninh mạng cho cán bộ, công chức, viên chức, người lao động khi tham gia hoạt động trên không gian mạng.

Các trường học xây dựng chương trình, kế hoạch học tập, rèn luyện kỹ năng tư duy, phản biện cho học sinh về an toàn, an ninh mạng đối với các thông tin sai lệch trên không gian mạng; tăng cường công tác phổ biến kiến thức, tình hình, xu hướng và các nguy cơ, hậu quả trong công tác an toàn, an ninh mạng của thế giới và trong nước để toàn thể cán bộ quản lý, giáo viên, nhân viên, học sinh và cha mẹ học sinh biết, thực hiện.

2.8. Đầu tư nguồn lực và bảo đảm kinh phí thực hiện

Bố trí đảm bảo nhân lực chuyên trách, chịu trách nhiệm về an toàn, an ninh mạng trong cơ quan, các trường học.

Đầu tư nguồn lực để xây dựng hệ thống kỹ thuật, thiết bị triển khai các hoạt động bảo đảm an toàn, an ninh mạng và trong hoạt động của cơ quan, các đơn vị trường học.

Bố trí chi kinh phí phục vụ công tác an toàn, an ninh mạng đạt tối thiểu theo quy định (10% kinh phí chi cho khoa học công nghệ, chuyển đổi số, ứng dụng công nghệ thông tin).

Bảo đảm kinh phí thực hiện các nhiệm vụ tại Kế hoạch này.

IV. TỔ CHỨC THỰC HIỆN

1. Phòng Giáo dục và Đào tạo các huyện, thị xã, thành phố

Theo dõi, đôn đốc các cơ sở giáo dục trực thuộc triển khai thực hiện các nhiệm vụ về an toàn thông tin mạng được giao tại Kế hoạch này.

Tăng cường kiểm tra, đánh giá đối với các cơ sở giáo dục trong công tác bảo đảm an ninh mạng, bảo vệ hạ tầng số, nền tảng số, dữ liệu cá nhân, bảo vệ hệ thống thông tin của các cơ quan Đảng, Nhà nước theo chức năng, nhiệm vụ.

Phối hợp các cơ quan, đơn vị liên quan triển khai thực hiện hiệu quả các chương trình, đề án đào tạo, phát triển nguồn nhân lực an ninh mạng, trong đó chú trọng đầu tư, xây dựng, phát triển lực lượng chuyên trách bảo vệ an ninh mạng đáp ứng thực tiễn, yêu cầu công tác.

Ưu tiên bố trí nguồn lực (nhân lực, kinh phí) và điều kiện để triển khai hoạt động bảo đảm an toàn, an ninh mạng trong hoạt động nội bộ của cơ quan, đơn vị và lĩnh vực quản lý.

Tổng hợp, kiến nghị và đề xuất cấp có thẩm quyền xem xét, chỉ đạo triển khai thực hiện các giải pháp về an ninh mạng cho phù hợp với tình hình thực tiễn trong quá trình thực hiện các nhiệm vụ được giao.

2. Các đơn vị trực thuộc Sở

Tổ chức, phối hợp triển khai thực hiện các nhiệm vụ được giao tại Kế hoạch này.

Ưu tiên bố trí nguồn lực (nhân lực, kinh phí) và điều kiện để triển khai hoạt động bảo đảm an toàn, an ninh mạng trong hoạt động nội bộ của cơ quan, đơn vị và lĩnh vực quản lý.

3. Chế độ thông tin, báo cáo

Căn cứ Kế hoạch này và chức năng, nhiệm vụ được giao, Thủ trưởng các cơ quan, đơn vị xây dựng kế hoạch triển khai thực hiện nghiêm túc; đảm bảo hình thành được lực lượng bảo đảm an toàn, an ninh mạng tại cơ quan, đơn vị, trong đó mỗi cơ quan, đơn vị có một bộ phận làm cán bộ đầu mối, chịu trách nhiệm về công tác đảm bảo an toàn, an ninh mạng. Định kỳ hằng năm (**trước ngày 20/10**), các đơn vị tổng hợp báo cáo (*về tình hình, kết quả triển khai thực hiện và khó khăn, vướng mắc, kiến nghị, đề xuất*) gửi về Sở GD&ĐT. Riêng danh sách cán bộ đầu mối phối hợp và Kế hoạch triển khai thực hiện, các đơn vị gửi về Sở GD&ĐT theo đường dẫn <https://forms.gle/D58TdKEtdX3YFqiv8> **trước ngày 19/5/2023** để theo dõi, tổng hợp.

Trong quá trình thực hiện, nếu có khó khăn, vướng mắc, các đơn vị kịp thời báo cáo về Sở GD&ĐT (qua phòng Quản lý chất lượng giáo dục) để được hướng dẫn hoặc tổng hợp, trình Chủ tịch UBND tỉnh xem xét, quyết định./.

Nơi nhận:

- UBND tỉnh (để b/c);
- Giám đốc, các Phó Giám đốc;
- Các phòng thuộc Sở;
- Phòng GD&ĐT các huyện, thị xã, thành phố;
- Các đơn vị trực thuộc Sở;
- Lưu: VT, QLCLGD_(Ph).

GIÁM ĐỐC