

Số: /KH-SGDĐT

Hưng Yên, ngày tháng 02 năm 2026

KẾ HOẠCH

Triển khai thực hiện Chương trình hành động số 09-CTr/TU của Tỉnh ủy về thực hiện Chỉ thị số 57-CT/TW của Ban Bí thư về tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu

Căn cứ Chỉ thị số 57-CT/TW ngày 31/12/2025 của Ban Bí thư Trung ương Đảng về tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu,

Thực hiện Chương trình hành động số 09-CTr/TU ngày 13/02/2026 của Tỉnh ủy về thực hiện Chỉ thị số 57-CT/TW của Ban Bí thư về tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu,

Căn cứ Công văn số 4079/UBND-NC ngày 30/12/2025 của UBND tỉnh về tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu trên địa bàn tỉnh;

Sở Giáo dục và Đào tạo xây dựng Kế hoạch triển khai tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu ngành giáo dục và đào tạo, với các nội dung như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích:

- Cụ thể hóa các mục tiêu, nhiệm vụ tại Chương trình hành động số 09-CTr/TU phù hợp với đặc thù ngành Giáo dục và Đào tạo.
- Nâng cao nhận thức, trách nhiệm của cán bộ quản lý, giáo viên, nhân viên và học sinh về an ninh mạng, an toàn thông tin.
- Bảo vệ tuyệt đối an toàn hệ thống dữ liệu ngành (CSDL ngành, Học bạ số, Cổng thông tin...) và bí mật nhà nước trong lĩnh vực giáo dục.

2. Yêu cầu:

- Bám sát nguyên tắc "An toàn, an ninh mạng là trọng tâm, xuyên suốt, không thể tách rời trong chuyển đổi số".
- Kết hợp chặt chẽ giữa đầu tư hạ tầng kỹ thuật với nâng cao kỹ năng số cho đội ngũ.
- 100% hệ thống thông tin, máy tính soạn thảo văn bản mật phải được kiểm soát chặt chẽ; khắc phục triệt để tình trạng lộ lọt tài khoản và dữ liệu cá nhân học sinh.

II. MỤC TIÊU CỤ THỂ

1. 100% hệ thống thông tin của Sở và các đơn vị trực thuộc được bảo vệ theo mô hình 4 lớp và được giám sát an toàn thông tin.

2. 100% dữ liệu dùng chung, dữ liệu chuyên ngành (Học bạ số, hồ sơ cán bộ...) được lưu trữ tập trung, chấm dứt tình trạng máy chủ phân tán không bảo đảm an toàn tại các đơn vị cấp cơ sở.

3. 100% máy tính soạn thảo văn bản mật không kết nối Internet.

III. NHIỆM VỤ VÀ GIẢI PHÁP TRỌNG TÂM

1. Tuyên truyền, nâng cao nhận thức và kỹ năng

- Tổ chức quán triệt sâu rộng Chỉ thị số 57-CT/TW và Chương trình 09-CTr/TU tới toàn thể cán bộ, đảng viên, công chức, viên chức.

- Lồng ghép thực hiện các nội dung tuyên truyền nâng cao nhận thức trong thực hiện Kế hoạch số 02/KH-SGDĐT ngày 08/01/2026 về chuyển đổi số năm 2026.

- Tiếp tục triển khai phong trào "Bình dân học vụ số" và các khóa tập huấn về kỹ năng số, an ninh mạng cho học sinh cấp THCS, THPT như đã thực hiện tại Kế hoạch 1176/KH-SGDĐT.

- Tăng cường giáo dục pháp luật, đạo đức, lối sống, kỹ năng ứng xử trên không gian mạng cho học sinh, sinh viên; phòng chống các thông tin xấu độc. Quán triệt cán bộ, giáo viên, nhân viên không chia sẻ tài khoản, mật khẩu các hệ thống thông tin (CSDL ngành, QLVB, Mail công vụ).

2. Bảo đảm an toàn hệ thống thông tin và dữ liệu

- Rà soát hạ tầng: Thực hiện nghiêm việc rà soát, đánh giá cấp độ an toàn hệ thống thông tin đối với các nền tảng số của ngành (Hệ thống quản lý trường học, Cổng thông tin, Học bạ số...) theo yêu cầu tại Công văn 3537/UBND-KGVX.

- Mô hình bảo vệ: Triển khai đầy đủ các giải pháp bảo vệ thiết bị đầu cuối (Endpoint Security), phần mềm phòng chống mã độc có bản quyền (như VNPT Smart IR,...) cho 100% máy tính công vụ.

- Tập trung dữ liệu: Phối hợp với Sở Khoa học và Công nghệ, Viettel Hưng Yên, VNPT Hưng Yên, Công ty Cổ phần phần mềm Quảng Ích để quy hoạch, đưa dữ liệu các trường học về lưu trữ tập trung tại Trung tâm dữ liệu của tỉnh hoặc hạ tầng đám mây đạt chuẩn, xóa bỏ các máy chủ vật lý đơn lẻ tại trường học không đảm bảo an toàn.

3. Công tác bảo vệ bí mật nhà nước (BMNN)

- Thực hiện nghiêm Nội quy bảo vệ bí mật nhà nước của Sở GDĐT (ban hành kèm Quyết định số 781/QĐ-SGDĐT ngày 24/10/2025).

- Tuyệt đối không kết nối Internet đối với máy tính dùng để soạn thảo, lưu trữ tài liệu chứa bí mật nhà nước (đề thi, hồ sơ nhân sự thuộc diện mật...).

- Triển khai giải pháp ký số văn bản và hệ thống quản lý văn bản mật theo hướng dẫn của Ban Cơ yếu Chính phủ và UBND tỉnh.

4. Ứng cứu sự cố an toàn thông tin

- Duy trì hoạt động hiệu quả của Đội ứng cứu sự cố an toàn thông tin mạng ngành GDĐT (đã thành lập theo Quyết định số 1211/QĐ-SGDĐT ngày 12/12/2025).

- Tổ chức trực giám sát 24/7 trong các đợt cao điểm (Kỳ thi tốt nghiệp THPT, tuyển sinh đầu cấp).

- Tổ chức diễn tập thực chiến ứng cứu sự cố định kỳ hằng năm theo Phương án số 2283/PA-SGDĐT.

- Phối hợp với Công an tỉnh, Sở Khoa học Công nghệ tham gia, tổ chức các cuộc diễn tập thực chiến trong năm 2026.

(Có danh mục nhiệm vụ trọng tâm thực hiện công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu gửi kèm theo)

IV. TỔ CHỨC THỰC HIỆN

1. Văn phòng Sở.

- Là cơ quan thường trực của Ban Chỉ đạo Chuyển đổi số và Đội ứng cứu sự cố an toàn thông tin mạng (ATTTM) của ngành. Quản trị, giám sát an toàn thông tin cho Cổng thông tin điện tử, Hệ thống quản lý văn bản, CSDL ngành.

- Chủ trì, phối hợp với Công an tỉnh (Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao PA05), Sở KHCN tổ chức kiểm tra, đánh giá an toàn thông tin định kỳ; tổ chức diễn tập ứng cứu sự cố không gian mạng hàng năm cho toàn ngành.

- Chủ trì tham mưu công tác Bảo vệ bí mật nhà nước (BMNN): Thường xuyên rà soát, kiểm tra an ninh, an toàn các máy tính dùng để soạn thảo văn bản mật (tuyệt đối không kết nối Internet); quản lý hệ thống sổ đăng ký, chuyển giao BMNN theo đúng quy định của Bộ Công an.

- Quản lý chặt chẽ việc cấp phát, thu hồi chứng thư chữ ký số chuyên dùng công vụ cho cán bộ, giáo viên.

- Chủ trì, phối hợp với các đơn vị liên quan tổ chức thanh tra, kiểm tra việc chấp hành các quy định pháp luật về an ninh mạng, bảo vệ bí mật nhà nước và bảo vệ dữ liệu cá nhân tại các cơ sở giáo dục trên địa bàn tỉnh; đề xuất xử lý nghiêm các tổ chức, cá nhân vi phạm.

2. Phòng Kế hoạch - Tài chính.

- Chủ trì tổng hợp, tham mưu lãnh đạo Sở và UBND tỉnh bố trí nguồn vốn ngân sách nhà nước hằng năm để thực hiện Kế hoạch.

- Bảo đảm ưu tiên phân bổ kinh phí cho công tác an toàn thông tin (đầu tư thiết bị tường lửa, phần mềm diệt mã độc có bản quyền, sao lưu dữ liệu độc lập) và triển khai Học bạ số, các hệ thống CSDL dùng chung theo đúng quy định phân cấp ngân sách.

3. Phòng Tổ chức cán bộ

- Tích hợp nội dung bồi dưỡng kiến thức, kỹ năng về an toàn, an ninh mạng, bảo vệ dữ liệu cá nhân vào các chương trình tập huấn, bồi dưỡng thường xuyên cho đội ngũ cán bộ quản lý, giáo viên, nhân viên toàn ngành.

- Rà soát, quản lý chặt chẽ và bảo mật dữ liệu hồ sơ nhân sự của cán bộ, công chức, viên chức trên phần mềm CSDL ngành và hệ thống quản lý CBCCVC; đảm bảo tuân thủ Luật Bảo vệ dữ liệu cá nhân.

4. Phòng Giáo dục Phổ thông và Phòng Giáo dục Mầm non

- Phòng GDPT: Chủ trì chỉ đạo các trường học triển khai an toàn hệ thống Học bạ số; hướng dẫn giáo viên sử dụng và bảo mật chữ ký số cá nhân trong việc ký duyệt học bạ điện tử, sổ điểm điện tử, không để xảy ra tình trạng ký thay, lộ lọt tài khoản.

- Chỉ đạo các cơ sở giáo dục lồng ghép, tích hợp nội dung giáo dục về kỹ năng công dân số, nhận diện thông tin xấu độc, kỹ năng an toàn trên không gian mạng vào chương trình học chính khóa và hoạt động ngoại khóa cho học sinh các cấp.

5. Phòng Quản lý chất lượng

- Chủ trì, chịu trách nhiệm tuyệt đối trong việc bảo đảm an ninh, an toàn, bảo mật dữ liệu của các phần mềm: Quản lý văn bằng, chứng chỉ, Quản lý thi tuyển sinh lớp 10, Hệ thống tuyển sinh đầu cấp và các kỳ thi học sinh giỏi.

- Thực hiện các quy trình bảo mật nghiêm ngặt (theo chuẩn bảo vệ bí mật nhà nước) trong công tác ra đề thi, in sao đề thi và quản lý phôi văn bằng, chứng chỉ điện tử.

6. Phòng Giáo dục nghề nghiệp - Giáo dục thường xuyên

- Làm đầu mối chủ trì triển khai phong trào "Bình dân học vụ số" sâu rộng trong cộng đồng; phối hợp tổ chức các khóa học bồi dưỡng nâng cao kiến thức về pháp luật an ninh mạng, an toàn giao thông trên không gian mạng và Trí tuệ nhân tạo (AI) cho học viên, người dân và người lao động.

- Kiểm soát an toàn thông tin đối với dữ liệu của Mô hình thi trực tuyến tập trung qua xác thực thẻ CCCD gắn chip (Mô hình 21).

8. Các cơ sở giáo dục trực thuộc Sở và cơ sở giáo dục trên địa bàn tỉnh

a) Trách nhiệm của Người đứng đầu (Hiệu trưởng/Giám đốc Trung tâm)

- Trực tiếp lãnh đạo, chỉ đạo và chịu trách nhiệm toàn diện về công tác an toàn, an ninh mạng tại đơn vị mình.

- Chịu trách nhiệm trước Giám đốc Sở GDĐT/đơn vị chủ quản và trước pháp luật nếu để xảy ra sự cố lộ, lọt dữ liệu cá nhân của học sinh, giáo viên (như điểm số, hồ sơ) do nguyên nhân chủ quan hoặc do buông lỏng quản lý.

- Đưa kết quả thực hiện công tác đảm bảo an toàn thông tin, an ninh mạng và chuyển đổi số thành một tiêu chí quan trọng để đánh giá, bình xét thi đua hằng năm của đơn vị và cá nhân.

b) Về quản lý tài khoản, mật khẩu và Cơ sở dữ liệu (CSDL)

- Chỉ định rõ cá nhân (viên chức CNTT hoặc văn thư) phụ trách quản trị hệ thống CSDL ngành của trường. Tuyệt đối không dùng chung tài khoản; yêu cầu toàn bộ giáo viên, nhân viên đặt mật khẩu có độ phức tạp cao đối với các phần mềm quản lý (SMAS, vnEdu, CSDL).

- Giao bộ phận phụ trách CNTT thường xuyên đôn đốc, kiểm tra việc thay đổi mật khẩu mặc định của cá nhân trong đơn vị.

- Thực hiện ngay biện pháp khóa tài khoản, hủy quyền truy cập trên các hệ thống thông tin đối với các cán bộ, giáo viên đã nghỉ hưu, thôi việc hoặc chuyển công tác để ngăn chặn nguy cơ xâm nhập, rò rỉ dữ liệu.

c) Về đảm bảo hạ tầng, phần mềm và Học bạ số

- Trang bị đầy đủ chứng thư chữ ký số cho cán bộ quản lý và giáo viên theo quy định để thực hiện ký duyệt hồ sơ điện tử, học bạ số.

- Ban hành quy chế nội bộ của trường quy định rõ trách nhiệm từng bộ phận, cá nhân trong việc quản lý, khai thác, sử dụng Hệ thống quản lý trường học và Học bạ số.

- Triển khai các giải pháp phòng chống mã độc, bảo đảm an toàn dữ liệu trên 100% thiết bị máy tính dùng chung và máy tính cá nhân dùng trong công vụ tại trường.

d) Về công tác tuyên truyền và giáo dục kỹ năng trên không gian mạng

- Thường xuyên tuyên truyền, nâng cao nhận thức, ý thức trách nhiệm cho cán bộ, giáo viên và học sinh; yêu cầu tuyệt đối không lan truyền, chia sẻ các thông tin, video, hình ảnh xấu độc, tiêu cực trên không gian mạng.

- Tăng cường đăng tải các thông tin chính thống, các gương điển hình tiên tiến, mô hình hiệu quả lên Cổng thông tin điện tử và mạng xã hội của nhà trường để định hướng dư luận và lan tỏa những giá trị tích cực của ngành.

9. Ủy ban nhân dân các xã, phường

Đề nghị UBND các xã, phường căn cứ chức năng, nhiệm vụ quản lý nhà nước tại địa phương theo mô hình chính quyền 02 cấp, phối hợp chặt chẽ với Sở Giáo dục và Đào tạo thực hiện các nhiệm vụ sau:

- Về quản lý, chỉ đạo chung: Phối hợp quản lý, chỉ đạo các cơ sở giáo dục (Mầm non, Tiểu học, Trung học cơ sở) trên địa bàn thực hiện nghiêm túc các quy định về bảo đảm an toàn thông tin, an ninh mạng và chuyển đổi số. Chịu trách nhiệm nếu để xảy ra tình trạng vi phạm pháp luật về an ninh mạng hoặc lộ lọt dữ liệu nghiêm trọng tại các cơ sở giáo dục thuộc thẩm quyền quản lý.

- Về đầu tư hạ tầng và bảo vệ Bí mật nhà nước: Quan tâm bố trí nguồn lực, kinh phí để mua sắm, nâng cấp thiết bị đầu cuối (máy tính, máy in, mạng nội bộ tách biệt hoàn toàn với mạng Internet) cho các cơ sở giáo dục để phục vụ công tác soạn thảo, lưu trữ văn bản có chứa nội dung Bí mật nhà nước (như đề thi, hồ sơ mật) theo đúng chỉ đạo tại Công văn số 3537/UBND-KGVX và Công văn 4079/UBND-NC của UBND tỉnh.

- Về quản trị Cơ sở dữ liệu (CSDL) ngành và Học bạ số:

+ Cử cán bộ làm đầu mối tiếp nhận bàn giao tài khoản, thực hiện phân quyền và quản trị an toàn dữ liệu trên các hệ thống thông tin, CSDL ngành giáo dục cho các trường trực thuộc.

+ Chỉ đạo các cơ sở giáo dục trên địa bàn triển khai Học bạ số theo đúng kế hoạch; đôn đốc, kiểm tra và hỗ trợ xác minh, chuẩn hóa thông tin học sinh, bảo đảm dữ liệu đưa lên hệ thống chính xác, an toàn và bảo mật.

- Về bảo vệ tài khoản và phòng chống mã độc: Phối hợp chỉ đạo, đôn đốc các trường học cài đặt đầy đủ phần mềm phòng chống mã độc có bản quyền; thường xuyên rà soát, yêu cầu cán bộ, giáo viên thay đổi mật khẩu mặc định, bảo mật tài khoản cá nhân và tài khoản quản trị các phần mềm quản lý (SMAS, vnEdu, HTTT quản lý giáo dục, hệ thống văn bản...) để tránh nguy cơ bị tin tặc xâm nhập.

- Về xử lý sự cố không gian mạng: Trình báo kịp thời với cơ quan Công an và các cơ quan chức năng khi phát hiện các vụ việc bị tấn công mạng, mất an toàn dữ liệu hoặc các dấu hiệu nghi vấn hành vi lệch chuẩn, bạo lực, vi phạm pháp luật trên không gian mạng liên quan đến giáo viên và học sinh trên địa bàn.

10. Trách nhiệm của các đơn vị cung cấp dịch vụ viễn thông, CNTT và giải pháp Chuyển đổi số (Viettel Hưng Yên, VNPT Hưng Yên, Tập đoàn Công nghệ Quảng Ích...)

Trên cơ sở các Thỏa thuận hợp tác toàn diện đã ký kết với Sở GDĐT, các doanh nghiệp cung cấp dịch vụ có trách nhiệm:

- Cam kết bảo mật tuyệt đối: Cam kết đảm bảo bí mật, an toàn tuyệt đối các thông tin, dữ liệu ngành giáo dục (CSDL học sinh, nhà giáo, học bạ số) và các dịch vụ được cung cấp; chịu trách nhiệm trước pháp luật và Sở GDĐT nếu để xảy ra sự cố lộ, lọt dữ liệu từ phía hệ thống do mình cung cấp.

- Hỗ trợ kỹ thuật và ứng cứu sự cố 24/7: Chịu trách nhiệm về mặt kỹ thuật, đảm bảo hỗ trợ kỹ thuật 24/7 (bao gồm cả ngày nghỉ, ngày lễ). Phải phối hợp chặt chẽ với Đội ứng cứu sự cố an toàn thông tin mạng của ngành GDĐT để khắc phục kịp thời các sự cố, lỗi phát sinh, ngăn chặn các cuộc tấn công mạng (như DDoS, Ransomware).

- Sao lưu và phục hồi dữ liệu: Triển khai các giải pháp dự phòng, sao lưu dữ liệu (Backup) định kỳ, độc lập (Offline) để đảm bảo hệ thống hoạt động liên tục; sẵn sàng khôi phục hoạt động bình thường của hệ thống giáo dục trong thời gian ngắn nhất sau khi gặp sự cố mất an toàn thông tin.

- Nâng cấp hệ thống và vá lỗ hổng: Chủ động rà soát, nâng cấp hệ thống phần mềm (như nâng cấp SMAS 4.0, vnEdu, Hệ thống thông tin quản lý giáo dục Hưng Yên) để đáp ứng mô hình chính quyền địa phương 2 cấp; thường xuyên cập nhật các bản vá lỗi bảo mật đối với các hệ điều hành, phần mềm ứng dụng nhằm khắc phục triệt để các lỗ hổng đã được công bố.

- Hỗ trợ tập huấn, nâng cao năng lực: Phối hợp với Sở GDĐT, các nhà trường tổ chức các lớp tập huấn, hướng dẫn sử dụng an toàn các phần mềm quản lý, ứng dụng chữ ký số chuyên dùng và kỹ năng phòng chống mã độc, bảo vệ dữ liệu cá nhân cho đội ngũ cán bộ, giáo viên

Trong quá trình thực hiện, nếu có vướng mắc các đơn vị chủ động liên hệ với Văn phòng Sở để được giải đáp, tư vấn và hỗ trợ./.

Nơi nhận:

- Ban thường vụ Tỉnh ủy Hưng Yên;
- UBND các xã/phường
- Lãnh đạo Sở;
- Các đơn vị thuộc Sở;
- Các đơn vị trực thuộc Sở;
- Các đơn vị, doanh nghiệp: Viettel Hưng Yên, VNPT Hưng Yên, Công ty Quảng Ích (để phối hợp);
- Lưu: VT.

**KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC**

Đỗ Minh Trí

PHỤ LỤC
DANH MỤC NHIỆM VỤ TRỌNG TÂM THỰC HIỆN CÔNG TÁC BẢO ĐẢM
AN NINH MẠNG, BẢO MẬT THÔNG TIN, AN NINH DỮ LIỆU TRONG
NGÀNH GIÁO DỤC VÀ ĐÀO TẠO HUNG YÊN

(Kèm theo Kế hoạch số: /KH-SGDĐT ngày /02/2026 của Sở GDĐT)

STT	Nhiệm vụ trọng tâm	Cơ quan, đơn vị chủ trì	Cơ quan, tổ chức phối hợp	Thời gian hoàn thành
I	Hoàn thiện thể chế và quy định nội bộ			
1	Rà soát, sửa đổi, bổ sung Quy chế bảo vệ bí mật nhà nước của ngành phù hợp với bối cảnh chuyển đổi số	Văn phòng Sở	Các phòng chuyên môn, đơn vị trực thuộc	Quý I/2026
2	Thực hiện quy trình "Phiếu trình duyệt và đề xuất độ mật" đối với 100% văn bản soạn thảo có chứa nội dung bí mật nhà nước	Thủ trưởng các cơ quan, đơn vị, cơ sở giáo dục	Cán bộ, công chức, viên chức được giao nhiệm vụ	Thường xuyên
II	Bảo đảm an toàn hệ thống thông tin và dữ liệu số			
3	Triển khai cài đặt phần mềm phòng chống mã độc có bản quyền (VNPT Smart IR,...) cho 100% máy tính công vụ	Thủ trưởng các cơ sở giáo dục; Văn phòng Sở	VNPT Hưng Yên; UBND cấp xã	Trước 30/3/2026
4	Bảo vệ, quản trị an toàn dữ liệu Học bạ số, CSDL ngành; không để xảy ra lộ lọt dữ liệu cá nhân học sinh, giáo viên	Phòng GDPT, GDMN, QLCL; Thủ trưởng các cơ sở giáo dục	Viettel, VNPT, Tập đoàn Quảng Ích, UBND cấp xã	Thường xuyên / Theo năm học
5	Tích hợp yếu tố an toàn thông tin "ngay từ thiết kế" đối với các nền tảng số, hệ thống quản lý trường học; Chuyển đổi hạ tầng Cloud	Các doanh nghiệp cung cấp dịch vụ CNTT (Viettel, VNPT, Quảng Ích...)	Văn phòng Sở; Ban Chỉ đạo Chuyển đổi số ngành	Theo tiến độ từng dự án / Thường xuyên
III	Bảo đảm an ninh mạng và bảo vệ bí mật nhà nước			
6	Bố trí máy tính chuyên dụng dùng để soạn thảo, lưu trữ tài liệu mật đảm bảo tuyệt đối không kết nối Internet	Thủ trưởng các đơn vị trực thuộc; Hiệu trưởng các nhà trường	Văn phòng Sở; UBND cấp xã	Quý I/2026 và duy trì thường xuyên
7	Kết nối, sử dụng Mạng truyền số liệu chuyên dùng để phục vụ công tác gửi/nhận văn bản Mật	Văn phòng Sở	Sở KHCN; Các doanh nghiệp Viễn thông	Thường xuyên
IV	Ứng cứu sự cố an toàn thông tin mạng			
8	Duy trì hoạt động giám sát,	Văn phòng Sở	Các thành viên	Thường

STT	Nhiệm vụ trọng tâm	Cơ quan, đơn vị chủ trì	Cơ quan, tổ chức phối hợp	Thời gian hoàn thành
	trực 24/7 của Đội ứng cứu sự cố an toàn thông tin mạng ngành GDĐT (đặc biệt trong các kỳ thi)	(Đơn vị Thường trực)	Đội ứng cứu; Các doanh nghiệp viễn thông, CNTT	xuyên
9	Tổ chức diễn tập thực chiến ứng cứu sự cố không gian mạng cấp ngành	Văn phòng Sở	Công an tỉnh (PA05); Sở KHCN	Hằng năm
V	Tuyên truyền, đào tạo và đảm bảo nguồn lực			
10	Tập huấn kiến thức, nâng cao nhận thức về an toàn, an ninh mạng, bảo vệ dữ liệu cá nhân cho cán bộ, giáo viên, học sinh	Phòng Tổ chức cán bộ; Thủ trưởng các cơ sở giáo dục	Phòng GDNN-GDTX; Tỉnh đoàn; Công an tỉnh	Thường xuyên
11	Bố trí kinh phí đảm bảo an toàn thông tin, an ninh mạng (tối thiểu 10% tổng kinh phí CNTT/Chuyển đổi số)	Phòng Kế hoạch - Tài chính	Sở Tài chính; UBND cấp xã	Kế hoạch dự toán hằng năm