

QUYẾT ĐỊNH

**Ban hành Quy chế bảo đảm an ninh mạng, an toàn thông tin
đối với hệ thống thông tin thuộc phạm vi quản lý
của Trường THPT Trần Văn Lan**

HIỆU TRƯỞNG TRƯỜNG THPT TRẦN VĂN LAN

*Căn cứ Luật An ninh mạng số 116/2025/QH15 ngày 10 tháng 12 năm 2025;
Căn cứ Luật Chuyển đổi số số 148/2025/QH15 ngày 11 tháng 12 năm 2025;
Căn cứ Luật Dữ liệu số 60/2024/QH15 ngày 30 tháng 11 năm 2024;
Căn cứ Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 ngày 26 tháng 6 năm 2025 và Nghị định số 356/2025/NĐ-CP ngày 31 tháng 12 năm 2025 của Chính phủ;
Căn cứ Luật Bảo vệ bí mật nhà nước số 117/2025/QH15 ngày 10 tháng 12 năm 2025 và Nghị định số 63/2026/NĐ-CP ngày 28 tháng 02 năm 2026 của Chính phủ;
Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ và Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP;
Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc; Thông tư số 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 quy định hoạt động giám sát an toàn hệ thống thông tin;
Căn cứ Quyết định số 14/2026/QĐ-UBND ngày 30 tháng 01 năm 2026 của Ủy ban nhân dân tỉnh Ninh Bình ban hành Quy chế bảo đảm an ninh mạng, an toàn thông tin đối với hệ thống thông tin trên địa bàn tỉnh Ninh Bình;
Căn cứ Quyết định số 363/QĐ-SGDĐT ngày 04 tháng 3 năm 2026 của Sở Giáo dục và Đào tạo tỉnh Ninh Bình ban hành Quy chế bảo đảm an ninh mạng, an toàn thông tin đối với hệ thống thông tin thuộc phạm vi quản lý của Sở Giáo dục và Đào tạo;
Căn cứ Thông tư số 15/2026/TT-BGDĐT ngày 24 tháng 3 năm 2026 của Bộ trưởng Bộ Giáo dục và Đào tạo ban hành Điều lệ trường tiểu học, trường trung học cơ sở, trường trung học phổ thông và trường phổ thông có nhiều cấp học;
Theo đề nghị của Tổ trưởng Văn phòng và người phụ trách công nghệ thông tin của Trường THPT Trần Văn Lan.*

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an ninh mạng, an toàn thông tin đối với hệ thống thông tin thuộc phạm vi quản lý của Trường THPT Trần Văn Lan.

Điều 2. Quyết định này có hiệu lực kể từ ngày ký. Các quy định nội bộ trước đây của Nhà trường trái với Quyết định này hết hiệu lực thi hành.

Điều 3. Tập thể lãnh đạo trường, Tổ trưởng Văn phòng, tổ trưởng các tổ chuyên môn, Ban Biên tập Trang thông tin điện tử, người phụ trách công nghệ thông tin, quản trị viên các hệ thống, viên chức, người lao động, học sinh và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:

- Như Điều 3;
- Sở GDĐT Ninh Bình (để báo cáo);
- Tập thể lãnh đạo trường;
- Các tổ, bộ phận thuộc trường;
- Lưu: VT, VP.



QUY CHẾ

Bảo đảm an ninh mạng, an toàn thông tin đối với hệ thống thông tin thuộc phạm vi quản lý của Trường THPT Trần Văn Lan

(Ban hành kèm theo Quyết định số 214 /QĐ-THPTTVL ngày 17 tháng 9 năm 2026 của Hiệu trưởng Trường THPT Trần Văn Lan)

Chương I

QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. Quy chế này quy định việc bảo đảm an ninh mạng, an toàn thông tin đối với hạ tầng kỹ thuật, thiết bị, tài khoản, phần mềm, dữ liệu và các hệ thống thông tin do Trường THPT Trần Văn Lan trực tiếp quản lý hoặc được cơ quan có thẩm quyền cấp quyền khai thác, sử dụng.

2. Đối tượng áp dụng gồm Tập thể lãnh đạo trường; viên chức, người lao động; Ban Biên tập Trang thông tin điện tử; người phụ trách công nghệ thông tin; quản trị viên hệ thống; học sinh và tổ chức, cá nhân có liên quan khi truy cập, vận hành, khai thác hoặc xử lý dữ liệu của Nhà trường.

3. Đối với hệ thống thông tin dùng chung do Bộ Giáo dục và Đào tạo, UBND tỉnh, Sở Giáo dục và Đào tạo hoặc đơn vị khác làm chủ quản, Nhà trường thực hiện theo quy chế, phân quyền và phương án bảo vệ của chủ quản hệ thống; Quy chế này áp dụng đối với trách nhiệm nội bộ của Nhà trường và người sử dụng.

Điều 2. Hệ thống thông tin và dữ liệu thuộc phạm vi quản lý

1. Hệ thống thuộc phạm vi Quy chế gồm: mạng nội bộ, mạng không dây, máy tính và thiết bị số của Nhà trường; Hệ thống Quản lý văn bản và điều hành; thư điện tử công vụ; Trang thông tin điện tử; kho dữ liệu điện tử dùng chung; phần mềm/cơ sở dữ liệu ngành; hệ thống học bạ số; hệ thống tài chính - kế toán, tài sản và các hệ thống khác được Nhà trường sử dụng để thực hiện nhiệm vụ.

2. Dữ liệu thuộc phạm vi bảo vệ gồm dữ liệu người học, viên chức, tài chính, tài sản, văn bản điện tử, dữ liệu chuyên môn, dữ liệu định danh, dữ liệu y tế học đường, tư vấn học đường, dữ liệu hình ảnh và các dữ liệu khác do Nhà trường tạo lập, tiếp nhận hoặc quản lý.

3. Thiết bị/hệ thống camera, kiểm soát ra vào, thiết bị IoT hoặc thiết bị khác có kết nối mạng của Nhà trường (nếu có) được quản lý theo Quy chế này.

Điều 3. Nguyên tắc bảo đảm an ninh mạng, an toàn thông tin

1. Bảo đảm an ninh mạng là trách nhiệm của mọi cá nhân sử dụng hệ thống, không chỉ của người phụ trách công nghệ thông tin.

2. Thực hiện nguyên tắc quyền tối thiểu cần thiết, đúng người - đúng việc - đúng thời hạn; tài khoản và quyền truy cập phải gắn với vị trí, nhiệm vụ được giao.

3. Bảo vệ đồng thời tính bí mật, tính toàn vẹn, tính sẵn sàng và khả năng truy xuất của dữ liệu; ưu tiên phòng ngừa, phát hiện sớm, xử lý nhanh và khôi phục hoạt động.

4. Hệ thống, dịch vụ mới hoặc thay đổi lớn phải được xem xét yêu cầu an ninh mạng, bảo vệ dữ liệu trước khi đưa vào sử dụng.

5. Việc xử lý dữ liệu cá nhân phải đúng mục đích, đúng phạm vi cần thiết; dữ liệu bí mật nhà nước thực hiện theo pháp luật chuyên ngành.

Điều 4. Các hành vi bị nghiêm cấm

1. Truy nhập trái phép, chiếm quyền, phá hoại, làm gián đoạn hệ thống; cố ý thay đổi, xóa, sao chép, tiết lộ dữ liệu trái thẩm quyền.

2. Cho mượn, dùng chung tài khoản cá nhân, mật khẩu, mã xác thực, chứng thư chữ ký số; giả mạo người dùng hoặc sử dụng tài khoản của người khác.

3. Tự ý cài phần mềm không rõ nguồn gốc; vô hiệu hóa phần mềm bảo vệ; kết nối thiết bị lạ, thiết bị lưu trữ có nguy cơ mất an toàn vào hệ thống.

4. Đưa bí mật nhà nước, dữ liệu cá nhân nhạy cảm, hồ sơ học sinh, đề kiểm tra/đề thi chưa công bố, thông tin tài chính hoặc dữ liệu nội bộ hạn chế lên dịch vụ công cộng, mạng xã hội, nền tảng trí tuệ nhân tạo hoặc kho lưu trữ cá nhân khi chưa được phép và chưa có biện pháp bảo vệ phù hợp.

5. Che giấu sự cố, tự ý xóa nhật ký/băng chứng, ngăn cản hoạt động kiểm tra, giám sát hoặc thực hiện hành vi khác bị pháp luật nghiêm cấm.

Chương II

QUẢN LÝ THIẾT BỊ, TÀI KHOẢN, MẠNG VÀ DỮ LIỆU

Điều 5. Quản lý tài sản công nghệ thông tin

1. Tổ Văn phòng phối hợp người phụ trách công nghệ thông tin lập và cập nhật danh sách thiết bị, phần mềm, tài khoản quản trị, hệ thống và dịch vụ số Nhà trường đang sử dụng; xác định người quản lý và mục đích sử dụng.

2. Cá nhân được giao thiết bị có trách nhiệm bảo quản, khóa thiết bị khi rời vị trí, không tự ý tháo lắp, chuyển giao, thay đổi cấu hình quản trị hoặc mang thiết bị ra khỏi trường khi chưa được phép.

3. Khi sửa chữa, điều chuyển, thanh lý thiết bị có lưu dữ liệu phải sao lưu dữ liệu cần thiết và xóa dữ liệu an toàn trước khi bàn giao cho bên ngoài.

4. Khi cá nhân thay đổi nhiệm vụ, nghỉ dài hạn, chuyển công tác hoặc thôi việc phải bàn giao thiết bị, dữ liệu, tài khoản quản trị và quyền truy cập theo quy định.

Điều 6. Sử dụng máy tính và thiết bị cá nhân

1. Máy tính phục vụ công việc phải được cập nhật hệ điều hành, trình duyệt và phần mềm; cài đặt giải pháp phòng, chống mã độc phù hợp; không sử dụng phần mềm bẻ khóa hoặc không rõ nguồn gốc.

2. Thiết bị cá nhân chỉ được kết nối vào mạng nội bộ để xử lý công việc khi thật sự cần thiết và phải tuân thủ yêu cầu an ninh mạng của Nhà trường; không lưu lâu dài dữ liệu nhạy cảm trên thiết bị cá nhân.

3. Thiết bị dùng chung phải có tài khoản/phân quyền phù hợp; không bật lưu mật khẩu tự động cho các hệ thống nghiệp vụ; người dùng phải đăng xuất sau khi sử dụng.

4. Thiết bị dùng để xử lý bí mật nhà nước phải đáp ứng đầy đủ yêu cầu riêng của pháp luật về bảo vệ bí mật nhà nước; không sử dụng thiết bị kết nối Internet để soạn thảo, lưu trữ bí mật nhà nước trái quy định.

Điều 7. Quản lý phần mềm, thiết bị lưu trữ và tệp tin

1. Chỉ cài đặt phần mềm có nguồn gốc rõ ràng, hợp pháp và phục vụ công việc; việc cài đặt phần mềm có quyền quản trị hệ thống phải được người phụ trách công nghệ thông tin kiểm tra.

2. Tệp đính kèm, liên kết, USB/ổ lưu trữ ngoài phải được kiểm tra trước khi mở hoặc kết nối; không mở tệp/link đáng ngờ từ nguồn không xác định.

3. Tệp chứa dữ liệu cá nhân, thông tin nội bộ quan trọng phải được lưu ở kho được Nhà trường cho phép; khi cần gửi phải giới hạn người nhận, thời gian truy cập và áp dụng biện pháp bảo vệ phù hợp.

4. Không sao chép dữ liệu toàn trường hoặc dữ liệu hàng loạt sang USB, ổ cứng cá nhân, tài khoản đám mây cá nhân nếu chưa được người có thẩm quyền cho phép.

Điều 8. Quản lý tài khoản, mật khẩu và xác thực

1. Tài khoản cá nhân phải gắn với một người sử dụng; không tạo tài khoản dùng chung cho hoạt động có yêu cầu truy vết, ký số, phê duyệt hoặc quản trị.

2. Mật khẩu phải có tối thiểu 8 ký tự, gồm chữ hoa, chữ thường, số và ký tự đặc biệt; không sử dụng mật khẩu mặc định, mật khẩu dễ đoán hoặc dùng một mật khẩu cho nhiều hệ thống quan trọng.

3. Thay đổi mật khẩu tối thiểu 06 tháng/lần hoặc ngay khi có dấu hiệu lộ lọt; bật xác thực nhiều yếu tố đối với hệ thống có hỗ trợ, ưu tiên tài khoản quản trị, thư điện tử công vụ, kho dữ liệu và Trang thông tin điện tử.

4. Quyền truy cập phải được rà soát đầu năm học, khi thay đổi phân công và ít nhất mỗi học kỳ; tài khoản không còn nhu cầu phải khóa/thu hồi kịp thời.

5. Tài khoản quản trị phải tách khỏi tài khoản sử dụng thông thường khi hệ thống cho phép.

Điều 9. Quản lý mạng nội bộ và mạng không dây

1. Thiết bị mạng, bộ phát Wi-Fi, modem, bộ định tuyến phải thay mật khẩu quản trị mặc định, cập nhật phần mềm điều khiển khi có bản vá phù hợp và hạn chế truy cập giao diện quản trị từ bên ngoài.

2. Khi hạ tầng cho phép, tách hoặc phân quyền giữa mạng phục vụ quản trị/nghiệp vụ với mạng dành cho học sinh, khách; không sử dụng mạng khách để quản trị hệ thống nhạy cảm.

3. Không tự ý lắp thêm bộ phát Wi-Fi, thiết bị chuyển mạch, camera, thiết bị IoT hoặc đường truyền vào mạng Nhà trường khi chưa được phép.

4. Người phụ trách công nghệ thông tin theo dõi thiết bị kết nối bất thường và phối hợp xử lý khi phát hiện dấu hiệu quét mạng, tấn công, chiếm dụng băng thông hoặc truy cập trái phép.

Điều 10. Thư điện tử công vụ, kho dữ liệu dùng chung và dịch vụ đám mây

1. Ưu tiên sử dụng thư điện tử công vụ, hệ thống quản lý văn bản và kho dữ liệu được Nhà trường/cơ quan quản lý cho phép để trao đổi tài liệu công việc.

2. Không tự động chuyển tiếp thư công vụ sang hòm thư cá nhân; không gửi mật khẩu, mã OTP, khóa bí mật qua thư điện tử hoặc ứng dụng nhắn tin.

3. Kho dữ liệu dùng chung phải phân quyền theo thư mục, nhóm công việc; hạn chế quyền chia sẻ công khai; liên kết chia sẻ phải được thu hồi khi hết nhu cầu.

4. Tài liệu có dữ liệu cá nhân nhạy cảm, bí mật nhà nước hoặc hạn chế tiếp cận không được đưa lên dịch vụ đám mây công cộng nếu chưa đáp ứng điều kiện pháp lý và biện pháp bảo vệ cần thiết.

Điều 11. Sử dụng nền tảng trí tuệ nhân tạo và dịch vụ trực tuyến

1. Công cụ trí tuệ nhân tạo có thể được sử dụng hỗ trợ công việc khi phù hợp nhiệm vụ, nhưng người sử dụng phải chịu trách nhiệm kiểm tra kết quả và bảo vệ dữ liệu đầu vào.

2. Không nhập, tải lên hoặc chia sẻ với công cụ trí tuệ nhân tạo công cộng các dữ liệu nhận diện học sinh, hồ sơ sức khỏe/tư vấn, hồ sơ nhân sự, dữ liệu tài chính chi tiết, mật khẩu, khóa bí mật, bí mật nhà nước, đề thi/đề kiểm tra chưa công bố và tài liệu nội bộ hạn chế, trừ khi được phép và có giải pháp bảo vệ phù hợp.

3. Khi cần sử dụng dữ liệu để phân tích/hỗ trợ, phải ưu tiên ẩn danh, giảm định danh, sử dụng dữ liệu giả lập hoặc dữ liệu tổng hợp.

4. Không sử dụng công cụ tự động để thực hiện thao tác quản trị hệ thống, phát hành văn bản, ký số hoặc sửa dữ liệu chính thức nếu chưa được phê duyệt.

Điều 12. Trang thông tin điện tử và các kênh truyền thông số chính thức

1. Việc quản trị Trang thông tin điện tử thực hiện đồng thời theo Quy định quản lý, vận hành và cập nhật Trang thông tin điện tử của Nhà trường.

2. Tài khoản quản trị phải được giới hạn cho người được phân công; bật xác thực nhiều yếu tố nếu nền tảng hỗ trợ; thay đổi mật khẩu khi thay đổi nhân sự hoặc có dấu hiệu mất an toàn.

3. Nội dung trước khi đăng phải được kiểm tra về thẩm quyền, dữ liệu cá nhân, hình ảnh học sinh, bí mật nhà nước và thông tin hạn chế tiếp cận.

4. Kênh mạng xã hội chính thức của Nhà trường (nếu có) phải có ít nhất hai người được giao quản lý để bảo đảm khả năng khôi phục tài khoản, nhưng không sử dụng chung mật khẩu cá nhân; việc phân quyền thực hiện theo chức năng của nền tảng.

Điều 13. Bảo vệ dữ liệu cá nhân và dữ liệu người học

1. Chỉ thu thập, sử dụng, chia sẻ dữ liệu cá nhân trong phạm vi cần thiết cho nhiệm vụ giáo dục, quản lý và nghĩa vụ pháp lý; không thu thập thêm dữ liệu nếu không có mục đích rõ ràng.

2. Dữ liệu học sinh, đặc biệt dữ liệu sức khỏe, tư vấn học đường, kỷ luật, hoàn cảnh, sổ định danh, thông tin liên hệ, hình ảnh và dữ liệu sinh trắc học (nếu có) phải được giới hạn quyền truy cập theo nhiệm vụ.

3. Khi cung cấp dữ liệu cho tổ chức/cá nhân bên ngoài phải có căn cứ pháp luật, yêu cầu hợp lệ hoặc sự đồng ý hợp lệ của chủ thể dữ liệu trong trường hợp pháp luật yêu cầu; chỉ cung cấp phần dữ liệu cần thiết.

4. Hồ sơ học bạ số thực hiện đồng thời Quy chế nội bộ về phân công trách nhiệm, phân quyền khai thác, sử dụng hệ thống học bạ số của Nhà trường.

Điều 14. Bảo vệ bí mật nhà nước và thông tin hạn chế tiếp cận

1. Việc xác định, soạn thảo, sao chụp, truyền nhận, lưu trữ, tiêu hủy tài liệu bí mật nhà nước thực hiện theo Luật Bảo vệ bí mật nhà nước và quy định liên quan.

2. Không gửi tài liệu bí mật nhà nước qua thư điện tử thông thường, mạng xã hội, ứng dụng nhắn tin, hệ thống hoặc thiết bị không đáp ứng điều kiện bảo vệ.

3. Tài liệu nội bộ chưa công khai, đề kiểm tra/đề thi chưa công bố, hồ sơ nhân sự, hồ sơ tài chính và dữ liệu khác có hạn chế tiếp cận phải được phân quyền và không chia sẻ vượt phạm vi nhiệm vụ.

Điều 15. Sao lưu, lưu trữ và phục hồi dữ liệu

1. Đối với dữ liệu Nhà trường trực tiếp quản lý, phải xác định dữ liệu quan trọng cần sao lưu và lịch sao lưu phù hợp; tối thiểu có bản sao dự phòng tách biệt với bản đang sử dụng đối với dữ liệu không thể khôi phục từ hệ thống cấp trên.

2. Dữ liệu quan trọng phải được kiểm tra khả năng phục hồi ít nhất 02 lần/năm học hoặc sau thay đổi lớn của hệ thống.

3. Bản sao lưu phải được phân quyền, mã hóa hoặc bảo vệ phù hợp; không lưu bản sao duy nhất trên cùng thiết bị với dữ liệu gốc.

4. Đối với hệ thống do cơ quan cấp trên/nhà cung cấp vận hành, người phụ trách công nghệ thông tin phải nắm rõ cơ chế sao lưu, phục hồi, xuất dữ liệu và đầu mối hỗ trợ.

Điều 16. Thuê dịch vụ công nghệ thông tin và hỗ trợ kỹ thuật bên ngoài

1. Hợp đồng/dịch vụ công nghệ thông tin có xử lý dữ liệu Nhà trường phải quy định rõ phạm vi truy cập, trách nhiệm bảo mật, bảo vệ dữ liệu cá nhân, sao lưu, thông báo sự cố, bàn giao/hoàn trả/xóa dữ liệu và trách nhiệm khi chấm dứt dịch vụ.

2. Tài khoản kỹ thuật của nhà cung cấp chỉ được cấp trong phạm vi cần thiết; quyền truy cập từ xa phải được kiểm soát, giới hạn thời gian và thu hồi khi hoàn thành hỗ trợ.

3. Không cung cấp cho nhà cung cấp mật khẩu cá nhân của viên chức; trường hợp cần hỗ trợ phải sử dụng cơ chế ủy quyền/tài khoản kỹ thuật riêng nếu hệ thống hỗ trợ.

4. Khi thay đổi nhà cung cấp, phải bảo đảm bàn giao dữ liệu, tài liệu kỹ thuật, quyền quản trị cần thiết và duy trì khả năng khai thác liên tục.

Chương III

PHÂN CÔNG TRÁCH NHIỆM

Điều 17. Trách nhiệm của Hiệu trưởng

1. Hiệu trưởng chịu trách nhiệm chung về bảo đảm an ninh mạng, an toàn thông tin trong phạm vi Nhà trường quản lý.
2. Phê duyệt phân công đầu mối, quản trị viên, danh sách quyền quản trị quan trọng; quyết định biện pháp xử lý sự cố nghiêm trọng và việc cung cấp dữ liệu diện rộng khi thuộc thẩm quyền.
3. Chỉ đạo bố trí kinh phí, thiết bị, dịch vụ và điều kiện cần thiết theo khả năng, đúng quy định; tổ chức kiểm tra, khắc phục tồn tại.
4. Chỉ đạo báo cáo Sở Giáo dục và Đào tạo và cơ quan có thẩm quyền khi xảy ra sự cố theo mức độ và quy định.

Điều 18. Trách nhiệm của Phó Hiệu trưởng được phân công phụ trách chuyển đổi số, công nghệ thông tin

1. Trực tiếp chỉ đạo triển khai Quy chế; phối hợp Tổ Văn phòng và người phụ trách công nghệ thông tin xây dựng kế hoạch, danh mục hệ thống, biện pháp bảo vệ và lịch kiểm tra.
2. Kiểm soát phân quyền các hệ thống thuộc lĩnh vực phụ trách; chỉ đạo rà soát việc cập nhật, sao lưu, bảo vệ dữ liệu và khắc phục lỗi hỏng.
3. Chủ trì xử lý nghiệp vụ khi sự cố ảnh hưởng dạy học, học bạ số, cơ sở dữ liệu ngành, Trang thông tin điện tử hoặc hệ thống quản trị Nhà trường.
4. Báo cáo Hiệu trưởng định kỳ và đột xuất về tình hình an ninh mạng, an toàn thông tin.

Điều 19. Trách nhiệm của Tổ Văn phòng và nhân sự hỗ trợ giáo dục phụ trách văn thư

1. Tổ trưởng Văn phòng phối hợp quản lý danh mục tài sản, tài khoản, hồ sơ bàn giao; theo dõi việc thực hiện yêu cầu bảo mật đối với khối hành chính.
2. Nhân sự hỗ trợ giáo dục phụ trách văn thư thực hiện yêu cầu an ninh mạng đối với Hệ thống Quản lý văn bản và điều hành, thư điện tử công vụ, chữ ký số, văn bản điện tử và hồ sơ lưu trữ; không cung cấp tài liệu vượt thẩm quyền.
3. Tổ Văn phòng phối hợp người phụ trách công nghệ thông tin thực hiện thu hồi quyền khi viên chức thay đổi nhiệm vụ, chuyển công tác, nghỉ việc; lưu hồ sơ sự cố và hồ sơ bàn giao theo Danh mục hồ sơ của Nhà trường.
4. Dữ liệu tài chính, tài sản, nhân sự do bộ phận chuyên môn tương ứng chịu trách nhiệm nội dung; Tổ Văn phòng phối hợp về quản lý hồ sơ và quyền truy cập.

Điều 20. Trách nhiệm của người phụ trách công nghệ thông tin và quản trị viên hệ thống

1. Người phụ trách công nghệ thông tin, quản trị viên do Hiệu trưởng phân công bằng văn bản; chịu trách nhiệm kỹ thuật trong phạm vi được giao, không mặc nhiên có quyền truy cập nội dung dữ liệu vượt nhiệm vụ.

2. Thực hiện cấu hình, cập nhật, sao lưu, phân quyền theo phê duyệt; theo dõi nhật ký, cảnh báo, dung lượng, thiết bị mạng; hỗ trợ xử lý sự cố và phối hợp nhà cung cấp.

3. Không tự ý cấp thêm quyền, thay đổi dữ liệu nghiệp vụ, xóa nhật ký hoặc che giấu sự cố; các thao tác quản trị quan trọng phải có khả năng truy vết.

4. Duy trì danh sách tài khoản quản trị, thiết bị mạng và đầu mối hỗ trợ; đề xuất thay thế, cập nhật khi thiết bị/phần mềm hết hỗ trợ hoặc có rủi ro cao.

Điều 21. Trách nhiệm của Ban Biên tập Trang thông tin điện tử và các bộ phận chuyên môn

1. Ban Biên tập chịu trách nhiệm an toàn tài khoản quản trị nội dung, kiểm tra dữ liệu trước đăng tải và phối hợp xử lý khi Trang thông tin điện tử có dấu hiệu bị tấn công, chèn nội dung lạ hoặc mất quyền quản trị.

2. Tổ chuyên môn, giáo viên chủ nhiệm, giáo viên bộ môn chỉ khai thác dữ liệu học sinh trong phạm vi nhiệm vụ; không lập kho dữ liệu cá nhân ngoài hệ thống Nhà trường khi không cần thiết.

3. Kế toán, y tế, tư vấn học đường và các bộ phận quản lý dữ liệu nhạy cảm có trách nhiệm phân quyền chặt chẽ, bảo vệ tệp làm việc và kiểm soát người nhận khi gửi dữ liệu.

4. Người đứng đầu/phụ trách từng bộ phận chịu trách nhiệm nhắc nhở, kiểm tra việc chấp hành trong phạm vi bộ phận.

Điều 22. Trách nhiệm của viên chức, người lao động và học sinh

1. Viên chức, người lao động phải tuân thủ Quy chế; bảo vệ tài khoản, thiết bị và dữ liệu được giao; chủ động cập nhật kiến thức, cảnh giác với lừa đảo, mã độc, giả mạo và tấn công xã hội.

2. Khi phát hiện thư/tin nhắn đáng ngờ, lộ mật khẩu, thiết bị thất lạc, tệp bị mã hóa, tài khoản bị chiếm, dữ liệu bị gửi nhầm hoặc hành vi truy cập bất thường phải báo ngay, không tự che giấu hoặc xử lý làm mất bằng chứng.

3. Học sinh khi sử dụng mạng, thiết bị hoặc tài khoản do Nhà trường cung cấp phải đúng mục đích học tập; không dò quét, phá hoại, vượt quyền, phát tán mã độc, truy cập trái phép hoặc chia sẻ tài khoản cho người khác.

4. Vi phạm tùy tính chất, mức độ được xử lý theo pháp luật, quy định của ngành và quy định nội bộ có liên quan.

Chương IV

GIÁM SÁT, QUẢN LÝ RỦI RO VÀ ỨNG CỨU SỰ CỐ

Điều 23. Rà soát rủi ro, lỗ hổng và bản vá

1. Người phụ trách công nghệ thông tin duy trì danh sách hệ thống, thiết bị, phiên bản phần mềm; theo dõi cảnh báo từ cơ quan quản lý, nhà cung cấp và nguồn tin cậy.

2. Lỗi hỏng nghiêm trọng phải được đánh giá và khắc phục sớm; ưu tiên hệ thống công khai trên Internet, tài khoản quản trị, thiết bị mạng và hệ thống chứa dữ liệu cá nhân.

3. Định kỳ ít nhất mỗi học kỳ kiểm tra tài khoản, thiết bị, cấu hình chia sẻ, phần mềm hết hỗ trợ và các quyền truy cập bất thường.

4. Việc kiểm thử/xâm nhập hệ thống chỉ được thực hiện khi có thẩm quyền và phạm vi được phê duyệt; nghiêm cấm tự ý thử công cụ tấn công trên hệ thống Nhà trường.

Điều 24. Phân loại và nguyên tắc ứng cứu sự cố

1. Sự cố mức thông thường: ảnh hưởng một thiết bị/tài khoản, chưa có dấu hiệu lan rộng hoặc lộ dữ liệu quan trọng; ưu tiên cô lập và xử lý tại chỗ.

2. Sự cố nghiêm trọng: ảnh hưởng nhiều thiết bị/tài khoản, hệ thống dạy học/quản trị bị gián đoạn, tài khoản quản trị bị chiếm, có dấu hiệu lộ dữ liệu cá nhân diện rộng, mất dữ liệu hoặc tấn công có chủ đích; phải báo ngay Hiệu trưởng và đầu mối cấp trên.

3. Sự cố liên quan bí mật nhà nước hoặc có dấu hiệu vi phạm pháp luật được xử lý theo quy định chuyên ngành và phối hợp cơ quan có thẩm quyền.

4. Nguyên tắc xử lý: ưu tiên an toàn con người và dữ liệu; cô lập để ngăn lan rộng; bảo toàn bằng chứng; khôi phục có kiểm soát; không trả tiền chuộc, thương lượng hoặc phát ngôn đối ngoại khi chưa được người có thẩm quyền quyết định.

Điều 25. Quy trình ứng cứu sự cố

1. Phát hiện và báo cáo: người phát hiện thông báo ngay cho người phụ trách công nghệ thông tin, Phó Hiệu trưởng phụ trách và Hiệu trưởng đối với dấu hiệu nghiêm trọng.

2. Cô lập và bảo toàn: ngắt kết nối thiết bị/hệ thống bị nghi nhiễm khi cần; không tự ý xóa tệp, cài lại máy hoặc xóa nhật ký trước khi thu thập thông tin cần thiết.

3. Đánh giá và ngăn chặn: xác định phạm vi ảnh hưởng, tài khoản/dữ liệu liên quan; khóa tài khoản, đổi thông tin xác thực, chặn kết nối hoặc áp dụng biện pháp kỹ thuật phù hợp.

4. Khắc phục và phục hồi: làm sạch, cập nhật, phục hồi từ bản sao an toàn; kiểm tra trước khi đưa hệ thống trở lại hoạt động.

5. Báo cáo và rút kinh nghiệm: lập biên bản/hồ sơ sự cố, nguyên nhân, biện pháp, kết quả; cập nhật biện pháp phòng ngừa và báo cáo cấp trên khi thuộc trường hợp phải báo cáo.

Điều 26. Bảo toàn nhật ký, bằng chứng và thông tin sự cố

1. Nhật ký hệ thống, thư điện tử, ảnh chụp màn hình, tệp nghi vấn, thời gian phát hiện, tài khoản liên quan và biên bản xử lý phải được lưu giữ phù hợp phục vụ kiểm tra, khắc phục và xác minh.

2. Chỉ người được giao nhiệm vụ mới được truy cập hồ sơ sự cố; không đăng tải thông tin sự cố lên mạng xã hội hoặc trao đổi ra ngoài phạm vi xử lý khi chưa được phép.

3. Trường hợp có dấu hiệu tội phạm hoặc vi phạm pháp luật, Nhà trường bảo toàn thông tin, chứng cứ và phối hợp cơ quan có thẩm quyền theo quy định.

Chương V

BẢO ĐẢM AN NINH MẠNG THEO CẤP ĐỘ, KIỂM TRA VÀ ĐÀO TẠO

Điều 27. Bảo đảm an ninh mạng theo cấp độ hệ thống thông tin

1. Đối với hệ thống Nhà trường trực tiếp là chủ quản, việc xác định cấp độ, hồ sơ và phương án bảo vệ thực hiện theo quy định hiện hành và hướng dẫn của Sở Giáo dục và Đào tạo/cơ quan chuyên trách.

2. Đối với hệ thống dùng chung do cơ quan cấp trên làm chủ quản, Nhà trường tuân thủ cấp độ và phương án bảo vệ đã được phê duyệt, không tự ý thay đổi kiến trúc hoặc cấu hình bảo mật thuộc phạm vi chủ quản.

3. Các hệ thống đã được xác định cấp độ trước ngày 01 tháng 7 năm 2026 tiếp tục thực hiện theo quy định chuyển tiếp của Luật An ninh mạng số 116/2025/QH15; Nhà trường phối hợp chủ quản để hoàn thiện yêu cầu mới trong thời hạn pháp luật quy định.

Điều 28. Kiểm tra, tự đánh giá và khắc phục

1. Hằng năm, Nhà trường tổ chức ít nhất 01 đợt tự kiểm tra tổng thể về an ninh mạng, an toàn thông tin; ngoài ra kiểm tra chuyên đề khi có sự cố, cảnh báo hoặc yêu cầu của cấp trên.

2. Nội dung kiểm tra gồm tối thiểu: tài khoản/quyền truy cập; cập nhật phần mềm; thiết bị mạng; sao lưu; dữ liệu cá nhân; website; hệ thống học bạ số; chữ ký số; kho dữ liệu dùng chung; hồ sơ thuê dịch vụ và khả năng ứng cứu sự cố.

3. Tồn tại phải được lập danh sách theo nguyên tắc rõ người, rõ việc, rõ thời gian, rõ kết quả và rõ trách nhiệm kiểm soát; vấn đề vượt thẩm quyền phải báo cáo Sở Giáo dục và Đào tạo.

4. Không yêu cầu giáo viên, nhân viên lập thêm hồ sơ hình thức; ưu tiên sử dụng nhật ký hệ thống, báo cáo kỹ thuật, biên bản kiểm tra và hồ sơ đã có làm minh chứng.

Điều 29. Tuyên truyền, tập huấn và diễn tập

1. Đầu năm học và khi có yêu cầu, Nhà trường tổ chức phổ biến tối thiểu các nội dung: nhận diện lừa đảo/phishing, bảo vệ tài khoản, dữ liệu cá nhân, sử dụng thiết bị an toàn, xử lý sự cố và sử dụng AI an toàn.

2. Người có quyền quản trị, quản lý dữ liệu nhạy cảm hoặc ký số được hướng dẫn chuyên sâu theo nhiệm vụ.

3. Khuyến khích tổ chức diễn tập tình huống thực tế như mất tài khoản, mã độc tống tiền, gửi nhầm dữ liệu, website bị chiếm quyền hoặc mất kết nối học bạ số; diễn tập không được gây rủi ro cho hệ thống đang vận hành.

Chương VI

TỔ CHỨC THỰC HIỆN

Điều 30. Chế độ báo cáo và hồ sơ quản lý

1. Người phụ trách công nghệ thông tin phối hợp Tổ Văn phòng lập hồ sơ quản lý an ninh mạng, an toàn thông tin gồm: danh mục hệ thống/thiết bị; danh sách tài khoản quản trị; biên bản bàn giao; kết quả kiểm tra; hồ sơ sự cố; báo cáo khắc phục và tài liệu liên quan.

2. Báo cáo định kỳ, đột xuất thực hiện theo yêu cầu của Sở Giáo dục và Đào tạo và cơ quan có thẩm quyền; sự cố nghiêm trọng phải báo cáo kịp thời, không chờ kỳ báo cáo.

3. Hồ sơ, tài liệu được bảo quản và nộp lưu theo Quy chế công tác văn thư, lưu trữ và Danh mục hồ sơ của Nhà trường.

Điều 31. Tổ chức thực hiện

1. Tổ Văn phòng và người phụ trách công nghệ thông tin tham mưu triển khai, hướng dẫn, theo dõi và đề xuất sửa đổi Quy chế.

2. Phó Hiệu trưởng được phân công phụ trách chuyển đổi số/công nghệ thông tin chịu trách nhiệm kiểm tra việc thực hiện trong các bộ phận; tổ trưởng, người phụ trách bộ phận tổ chức quán triệt đến từng thành viên.

3. Trong trường hợp văn bản pháp luật, quy định của UBND tỉnh hoặc Sở Giáo dục và Đào tạo được sửa đổi, bổ sung, thay thế thì thực hiện theo văn bản mới; Tổ Văn phòng tham mưu cập nhật Quy chế khi cần thiết.

4. Các nội dung chưa quy định tại Quy chế này thực hiện theo pháp luật về an ninh mạng, dữ liệu, bảo vệ dữ liệu cá nhân, bảo vệ bí mật nhà nước và quy định của cơ quan quản lý cấp trên.

PHỤ LỤC I
DANH MỤC NHÓM HỆ THỐNG THÔNG TIN VÀ TRÁCH NHIỆM BẢO VỆ
*(Kèm theo Quy chế bảo đảm an ninh mạng, an toàn thông tin
của Trường THPT Trần Văn Lan)*

Nhóm hệ thống/dữ liệu	Ví dụ tại Trường	Chủ quản/nguồn hệ thống	Đầu mối nội bộ	Kiểm soát tối thiểu
Điều hành - văn thư	Hệ thống Quản lý văn bản và điều hành; thư điện tử công vụ; chữ ký số	Cơ quan cấp trên/nhà cung cấp theo phân cấp	Tổ Văn phòng, Văn thư	Tài khoản cá nhân; MFA nếu có; kiểm tra văn bản; phân quyền; nhật ký; bàn giao/thu hồi
Dữ liệu giáo dục	CSDL ngành; học bạ số; dữ liệu học sinh; hệ thống tuyển sinh/chuyển trường	Bộ/Sở/đơn vị cung cấp theo hệ thống	PHT chuyên môn; GVCN; quản trị viên	Quyền theo lớp/môn; đối soát; bảo vệ định danh; ký số; lưu vết
Trang thông tin điện tử	Website/Trang thông tin điện tử của Trường	Nhà trường/đơn vị cung cấp	Ban Biên tập; quản trị viên	MFA; tài khoản riêng; cập nhật; sao lưu; kiểm duyệt dữ liệu cá nhân; xử lý chèn mã/nội dung lạ
Kho dữ liệu dùng chung	Kho tài liệu điện tử, thư mục dùng chung của Trường	Nhà trường/nền tảng được phép	Tổ Văn phòng; từng bộ phận	Phân quyền thư mục; không chia sẻ công khai mặc định; thu hồi liên kết; sao lưu dữ liệu quan trọng
Tài chính - tài sản	Phần mềm kế toán, kho bạc, hóa đơn/chứng từ điện tử, quản lý tài sản	Cơ quan có thẩm quyền/nhà cung cấp	Kế toán; Tổ Văn phòng	Tài khoản riêng; không chia sẻ chứng thư; giới hạn xuất dữ liệu; sao lưu hồ sơ
Hạ tầng mạng	Mạng LAN, Wi-Fi, modem/router, máy tính, máy in, thiết bị lưu trữ	Nhà trường	Người phụ trách CNTT	Đổi mật khẩu mặc định; cập nhật; chống mã độc; tách mạng khi có thể; kiểm kê thiết bị
Dữ liệu nhạy cảm chuyên biệt	Y tế học đường, tư vấn học đường, hồ sơ kỷ luật, hồ sơ viên chức	Nhà trường	Bộ phận phụ trách + Tổ Văn phòng	Quyền tối thiểu; mã hóa/bảo vệ tệp; hạn chế gửi; ghi nhận cung cấp/khai thác

Nhóm hệ thống/dữ liệu	Ví dụ tại Trường	Chủ quản/nguồn hệ thống	Đầu mối nội bộ	Kiểm soát tối thiểu
Thiết bị giám sát/IoT (nếu có)	Camera, thiết bị kiểm soát ra vào, thiết bị thông minh	Nhà trường/nhà cung cấp	Người phụ trách CNTT + bộ phận sử dụng	Đổi mật khẩu mặc định; giới hạn truy cập; cập nhật; kiểm soát thời gian lưu dữ liệu

PHỤ LỤC II
QUY TRÌNH XỬ LÝ NHANH SỰ CỐ AN NINH MẠNG, AN TOÀN THÔNG TIN

Bước	Người thực hiện chính	Nội dung tối thiểu
1. PHÁT HIỆN	Người phát hiện	Ghi nhận dấu hiệu: tài khoản bị chiếm, máy nhiễm mã độc, dữ liệu mất/sửa, gửi nhầm dữ liệu, website bị chèn nội dung, hệ thống ngừng hoạt động.
2. CÔ LẬP	Người phát hiện/Phụ trách CNTT	Ngắt kết nối thiết bị nghi nhiễm khi cần; khóa tài khoản có nguy cơ; không tự ý xóa dữ liệu, cài lại máy hoặc xóa nhật ký.
3. BÁO CÁO	Người phát hiện/Phụ trách CNTT	Báo ngay người phụ trách CNTT; đồng thời báo PHT phụ trách/Hiệu trưởng nếu ảnh hưởng nhiều người, dữ liệu nhạy cảm, tài khoản quản trị hoặc hoạt động của Trường.
4. ĐÁNH GIÁ - NGĂN CHẶN	Phụ trách CNTT + Lãnh đạo	Xác định phạm vi, tài khoản, thiết bị, dữ liệu liên quan; đổi thông tin xác thực, chặn truy cập/kết nối và phối hợp nhà cung cấp/cấp trên.
5. KHÔI PHỤC	Phụ trách CNTT + Nhà cung cấp	Làm sạch/cập nhật; phục hồi từ nguồn an toàn; kiểm tra dữ liệu, quyền và nhật ký trước khi đưa hệ thống trở lại hoạt động.
6. LẬP HỒ SƠ - RÚT KINH NGHIỆM	Tổ Văn phòng + Phụ trách CNTT	Lưu thời gian, bằng chứng, nguyên nhân, biện pháp, kết quả; báo cáo theo quy định; cập nhật biện pháp phòng ngừa.

Nguyên tắc nhớ nhanh: PHÁT HIỆN → CÔ LẬP → BÁO CÁO → NGĂN CHẶN → KHÔI PHỤC → LẬP HỒ SƠ. Không tự xử lý bằng cách xóa sạch dấu vết khi chưa đánh giá sự cố.

PHỤ LỤC III
BẢNG KIỂM TỰ RÀ SOÁT AN NINH MẠNG, AN TOÀN THÔNG TIN HÀNG
HỌC KỲ

TT	Nội dung kiểm tra	Kết quả	Biện pháp/Thời hạn khắc phục
1	Danh mục hệ thống, thiết bị, phần mềm và đầu mối quản lý đã được cập nhật.	☐ Đạt ☐ Chưa đạt ☐ KNA	
2	Tài khoản nghỉ việc/chuyển nhiệm vụ đã khóa hoặc thu hồi; quyền truy cập đã rà soát.	☐ Đạt ☐ Chưa đạt ☐ KNA	
3	Tài khoản quản trị, thư điện tử, website và kho dữ liệu quan trọng đã bật MFA nếu hệ thống hỗ trợ.	☐ Đạt ☐ Chưa đạt ☐ KNA	
4	Máy tính, trình duyệt, phần mềm chống mã độc và thiết bị mạng đã được cập nhật phù hợp.	☐ Đạt ☐ Chưa đạt ☐ KNA	
5	Không còn mật khẩu mặc định trên modem/router/Wi-Fi/camera/thiết bị quản trị.	☐ Đạt ☐ Chưa đạt ☐ KNA	
6	Kho dữ liệu dùng chung không có thư mục/tệp nhạy cảm đang chia sẻ công khai trái nhu cầu.	☐ Đạt ☐ Chưa đạt ☐ KNA	
7	Dữ liệu học sinh, nhân sự, y tế, tư vấn và tài chính được giới hạn đúng người sử dụng.	☐ Đạt ☐ Chưa đạt ☐ KNA	
8	Dữ liệu quan trọng đã có bản sao dự phòng; đã kiểm tra khả năng phục hồi.	☐ Đạt ☐ Chưa đạt ☐ KNA	
9	Trang thông tin điện tử và tài khoản truyền thông số không có tài khoản quản trị thừa.	☐ Đạt ☐ Chưa đạt ☐ KNA	
10	Các hợp đồng/dịch vụ CNTT có điều khoản bảo mật, dữ liệu và xử lý sự cố phù hợp.	☐ Đạt ☐ Chưa đạt ☐ KNA	
11	Nhật ký/cảnh báo/sự cố của học kỳ đã được rà soát; sự cố đã có hồ sơ khắc phục.	☐ Đạt ☐ Chưa đạt ☐ KNA	
12	Cán bộ, giáo viên, nhân viên đã được nhắc/tập huấn về phishing, mật khẩu, dữ liệu cá nhân và sử dụng AI an toàn.	☐ Đạt ☐ Chưa đạt ☐ KNA	