

Số: 328/QĐ-NTN

Thành phố Hồ Chí Minh, ngày 30 tháng 9 năm 2026

QUYẾT ĐỊNH

**Về việc ban hành Quy chế vận hành, quản trị hệ thống mạng
và an toàn thông tin tại Trường Tiểu học, THCS và THPT Ngô Thời Nhiệm**

HIỆU TRƯỞNG

TRƯỜNG TIỂU HỌC, THCS VÀ THPT NGÔ THỜI NHIỆM

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 trung học cơ sở, trường trung học phổ thông và trường phổ thông có nhiều cấp học;

Căn cứ Thông tư số 48/2026/TT-BGDĐT ngày 22 tháng 6 năm 2026 của Bộ Giáo dục và Đào tạo ban hành Quy chế tổ chức và hoạt động của trường tiểu học, trường trung học cơ sở, trường trung học phổ thông và trường phổ thông có nhiều cấp học loại hình tư thục;

Căn cứ Quyết định số 2424/QĐ-UBND ngày 07 tháng 6 năm 2008 của Chủ tịch Ủy ban Nhân dân Thành phố Hồ Chí Minh về cho phép sáp nhập trường Tiểu học dân lập Ngô Thời Nhiệm và Trường Trung học phổ thông Tư thục Ngô Thời Nhiệm thành trường Tiểu học, Trung học cơ sở và Trung học phổ thông Ngô Thời Nhiệm;

Căn cứ Luật Giáo dục số 43/2019/QH14 ngày 14 tháng 6 năm 2019 và các văn bản sửa đổi, bổ sung hiện hành;

Căn cứ Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 ngày 26 tháng 6 năm 2025;

Căn cứ Luật An ninh mạng số 116/2025/QH15 ngày 10 tháng 12 năm 2025;

Căn cứ Nghị định số 356/2025/NĐ-CP ngày 31 tháng 12 năm 2025 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Bảo vệ dữ liệu cá nhân;

Căn cứ Nghị định số 331/2026/NĐ-CP ngày 19 tháng 8 năm 2026 của Chính phủ về bảo vệ an ninh mạng đối với hệ thống thông tin;

Căn cứ Nghị định số 333/2026/NĐ-CP ngày 19 tháng 8 năm 2026 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật An ninh mạng;

Căn cứ Nghị định số 330/2026/NĐ-CP ngày 19 tháng 8 năm 2026 của Chính phủ quy định xử phạt vi phạm hành chính trong lĩnh vực an ninh mạng và bảo vệ dữ liệu cá nhân;

Căn cứ Quyết định số 1230/QĐ-SGDĐT ngày 08 tháng 5 năm 2024 của Sở Giáo dục và Đào tạo Thành phố Hồ Chí Minh ban hành Quy chế thu thập, quản lý, đồng bộ, chia sẻ dữ liệu ngành Giáo dục và Đào tạo Thành phố Hồ Chí Minh;

Căn cứ Kế hoạch số 245/KH-NTN ngày 08 tháng 9 năm 2026 của Trường Tiểu học, THCS và THPT Ngô Thời Nhiệm về Kế hoạch giáo dục nhà trường năm học 2026 - 2027;

Xét yêu cầu quản lý, vận hành hạ tầng công nghệ thông tin, chuyển đổi số và bảo đảm an toàn, an ninh mạng của Nhà trường.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế vận hành, quản trị hệ thống mạng và an toàn thông tin tại Trường Tiểu học, THCS và THPT Ngô Thời Nhiệm.

Điều 2. Quyết định này có hiệu lực kể từ ngày ký và thay thế Quyết định số 15/QĐ-NTN ngày 13 tháng 01 năm 2024 của Trường Tiểu học, THCS và THPT Ngô Thời Nhiệm về việc ban hành Quy chế vận hành, quản trị hệ thống mạng và an toàn thông tin tại Trường.

Điều 3. Các Phó Hiệu trưởng, Trưởng phòng Tổ chức - Hành chính và Pháp chế, bộ phận công nghệ thông tin, trưởng các đơn vị, tổ/nhóm chuyên môn, cán bộ quản lý, giáo viên, nhân viên, học sinh và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:

- Như Điều 3;
- Ban Lãnh đạo;
- Lưu: VT (HL) 



HUYỆU TRƯỞNG

Tưởng Nguyên Sự



**SỞ GIÁO DỤC VÀ ĐÀO TẠO
THANH PHỐ HỒ CHÍ MINH
TRƯỜNG TIỂU HỌC, THCS
VÀ THPT NGÔ THỜI NHIỆM**

**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc**

QUY CHẾ

Vận hành, quản trị hệ thống mạng và an toàn thông tin tại Trường Tiểu học, THCS và THPT Ngô Thời Nhiệm

*(Ban hành kèm theo Quyết định số 328/QĐ-NTN ngày 30 tháng 9 năm 2026 của
Hiệu trưởng Trường Tiểu học, THCS và THPT Ngô Thời Nhiệm)*

Chương I QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và mục tiêu

1. Quy chế này quy định nguyên tắc, trách nhiệm và yêu cầu trong quản lý, vận hành, sử dụng hệ thống mạng, hệ thống thông tin, nền tảng số, thiết bị công nghệ thông tin và bảo đảm an toàn, an ninh mạng tại Nhà trường.

2. Mục tiêu: bảo đảm hệ thống hoạt động ổn định, liên tục và an toàn; bảo vệ tính bí mật, toàn vẹn, sẵn sàng của thông tin; phòng ngừa, phát hiện và xử lý rủi ro, sự cố; quản lý hiệu quả tài sản công nghệ thông tin; nâng cao nhận thức, trách nhiệm của người sử dụng và phục vụ yêu cầu chuyển đổi số của Nhà trường.

Điều 2. Đối tượng áp dụng

Quy chế áp dụng đối với cán bộ quản lý, giáo viên, nhân viên, học sinh; các đơn vị, tổ/nhóm chuyên môn; nhà cung cấp, đối tác và tổ chức, cá nhân được phép kết nối, truy cập, khai thác hoặc quản trị hệ thống thông tin, mạng và thiết bị công nghệ thông tin thuộc phạm vi quản lý của Nhà trường.

Điều 3. Giải thích từ ngữ và nguyên tắc chung

1. Hệ thống thông tin của Nhà trường gồm hạ tầng mạng LAN/WAN/Wi-Fi/Internet; máy chủ, thiết bị mạng; hệ thống lưu trữ; website, thư điện tử, LMS, phần mềm quản lý nhà trường, cơ sở dữ liệu, hệ thống camera và các nền tảng số khác do Nhà trường quản lý hoặc thuê dịch vụ.

2. Tài khoản quản trị là tài khoản có quyền cấu hình, phân quyền, truy cập dữ liệu hoặc thay đổi hoạt động của hệ thống; phải được kiểm soát chặt chẽ hơn tài khoản người dùng thông thường.

3. Sự cố an toàn, an ninh mạng là sự kiện làm hoặc có nguy cơ làm mất tính bí mật, toàn vẹn, sẵn sàng của hệ thống, dữ liệu; bao gồm truy cập trái phép, rò rỉ dữ liệu, mã độc, lừa đảo, chiếm quyền tài khoản, tấn công mạng, mất dữ liệu và gián đoạn dịch vụ.

4. Việc vận hành hệ thống phải tuân thủ nguyên tắc đúng thẩm quyền, tối thiểu quyền cần thiết, có khả năng kiểm tra và truy vết; bảo đảm an toàn theo mức

độ rủi ro và tuân thủ pháp luật về an ninh mạng, bảo vệ dữ liệu cá nhân và quy định nội bộ của Nhà trường.

Chương II **TỔ CHỨC, PHÂN CÔNG VÀ TRÁCH NHIỆM**

Điều 4. Ban Giám hiệu

1. Chỉ đạo, phê duyệt chủ trương, quy chế, kế hoạch và nguồn lực về hạ tầng số, an toàn, an ninh mạng; quyết định các vấn đề vượt thẩm quyền của bộ phận công nghệ thông tin.

2. Chỉ đạo phân loại, rà soát hệ thống thông tin, đánh giá rủi ro và thực hiện các biện pháp bảo vệ phù hợp theo quy định pháp luật và điều kiện thực tế.

3. Chỉ đạo phối hợp xử lý sự cố nghiêm trọng; quyết định việc thông báo, báo cáo cơ quan có thẩm quyền khi thuộc trường hợp phải báo cáo theo quy định.

Điều 5. Bộ phận công nghệ thông tin

1. Là đầu mối kỹ thuật tham mưu và trực tiếp quản trị, vận hành hạ tầng mạng, máy chủ, thiết bị mạng, hệ thống lưu trữ, tài khoản, nền tảng số và các hệ thống được giao.

2. Xây dựng, cập nhật sơ đồ mạng, danh mục hệ thống, tài khoản quản trị, thiết bị, địa chỉ IP, cấu hình quan trọng và tài liệu kỹ thuật; quản lý thay đổi cấu hình có kiểm soát.

3. Thiết lập phân quyền, xác thực, sao lưu, nhật ký, giám sát; triển khai cập nhật bản vá, phòng chống mã độc, tường lửa và các biện pháp kỹ thuật phù hợp.

4. Tiếp nhận, phân loại, xử lý sự cố; bảo toàn nhật ký, chứng cứ điện tử cần thiết; báo cáo Ban Giám hiệu đối với sự cố nghiêm trọng hoặc có dấu hiệu vi phạm pháp luật.

5. Hỗ trợ người dùng; tổ chức hoặc phối hợp tập huấn về sử dụng hệ thống và an toàn thông tin; định kỳ tổng hợp tình trạng vận hành, rủi ro và đề xuất cải tiến.

6. Việc phân công cụ thể cho nhân sự phụ trách hạ tầng, thiết bị, website, dữ liệu số, hỗ trợ người dùng được Trưởng bộ phận công nghệ thông tin thực hiện theo vị trí việc làm và yêu cầu thực tế, không làm thay đổi trách nhiệm chung của bộ phận.

Điều 6. Các phòng, bộ phận, tổ/nhóm chuyên môn và người sử dụng

1. Trưởng các đơn vị chịu trách nhiệm phối hợp quản lý tài khoản, quyền truy cập và thiết bị được giao; thông báo kịp thời khi có thay đổi nhân sự hoặc nhu cầu phân quyền.

2. Cán bộ, giáo viên, nhân viên sử dụng hệ thống đúng mục đích; bảo vệ tài khoản, mật khẩu, dữ liệu và thiết bị; không tự ý cài phần mềm không rõ nguồn gốc, can thiệp cấu hình hoặc chia sẻ quyền truy cập.

3. Học sinh sử dụng mạng, thiết bị và tài khoản do Nhà trường cấp cho mục đích học tập và hoạt động giáo dục; không truy cập, phát tán nội dung vi phạm pháp luật, độc hại hoặc không phù hợp lứa tuổi; không tìm cách vượt biện pháp kiểm soát của Nhà trường.

4. Khi phát hiện dấu hiệu bất thường, mất tài khoản, lộ mật khẩu, thư lừa đảo, mã độc, rò rỉ dữ liệu hoặc sự cố thiết bị, người sử dụng phải ngừng thao tác có nguy cơ làm sự cố lan rộng và báo ngay cho bộ phận công nghệ thông tin.

Chương III **VẬN HÀNH VÀ QUẢN TRỊ HỆ THỐNG**

Điều 7. Quản lý tài khoản và xác thực

1. Mỗi người dùng sử dụng tài khoản định danh theo quy định; việc cấp mới, thay đổi, khóa hoặc thu hồi tài khoản phải gắn với chức năng, nhiệm vụ và tình trạng học tập, làm việc.

2. Tài khoản quản trị phải tách biệt với tài khoản sử dụng thông thường khi điều kiện kỹ thuật cho phép; hạn chế số lượng người có quyền quản trị và ghi nhận việc cấp quyền.

3. Áp dụng mật khẩu mạnh và xác thực đa yếu tố đối với tài khoản quản trị, thư điện tử, hệ thống chứa dữ liệu quan trọng hoặc dữ liệu cá nhân khi nền tảng hỗ trợ; nghiêm cấm dùng chung tài khoản quản trị nếu không có cơ chế kiểm soát và truy vết.

4. Khi cán bộ, giáo viên, nhân viên nghỉ việc, chuyển nhiệm vụ hoặc học sinh thôi học/chuyển trường, đơn vị phụ trách phải thông báo để điều chỉnh hoặc thu hồi quyền truy cập kịp thời.

Điều 8. Quản lý truy cập và phân quyền

1. Quyền truy cập được cấp theo nguyên tắc tối thiểu cần thiết và đúng phạm vi nhiệm vụ; định kỳ rà soát, thu hồi quyền không còn nhu cầu.

2. Không tự ý cung cấp dữ liệu, tài khoản, cấu hình, đường dẫn quản trị hoặc thông tin kỹ thuật nội bộ cho bên ngoài.

3. Truy cập từ xa vào hệ thống quản trị phải sử dụng phương thức an toàn do bộ phận công nghệ thông tin cho phép; hạn chế quản trị hệ thống qua mạng công cộng không tin cậy.

4. Việc giám sát truy cập, nhật ký và lưu lượng mạng chỉ thực hiện trong phạm vi cần thiết để vận hành, bảo mật, điều tra sự cố và tuân thủ pháp luật; không sử dụng dữ liệu giám sát ngoài mục đích hợp pháp.

Điều 9. Quản lý cấu hình, thay đổi, bản vá và phần mềm

1. Các cấu hình quan trọng phải được ghi nhận, sao lưu và thay đổi có kiểm soát; thay đổi có nguy cơ ảnh hưởng diện rộng phải được đánh giá trước và có phương án khôi phục.

2. Hệ điều hành, ứng dụng, firmware và thiết bị mạng phải được cập nhật bản vá phù hợp; ưu tiên xử lý lỗ hổng có mức rủi ro cao.

3. Chỉ cài đặt phần mềm hợp pháp, có nguồn gốc rõ ràng và cần thiết cho công việc; không sử dụng phần mềm bẻ khóa, công cụ vượt kiểm soát hoặc phần mềm có nguy cơ gây mất an toàn.

4. Các dịch vụ, cổng kết nối, tài khoản mặc định và chức năng không cần thiết phải được vô hiệu hóa hoặc hạn chế.

Điều 10. Quản lý mạng không dây, thiết bị cá nhân và thiết bị ngoại vi

1. Hệ thống Wi-Fi được phân tách, cấu hình và kiểm soát phù hợp theo nhóm người dùng và mục đích sử dụng; mật khẩu quản trị thiết bị mạng không được công khai.

2. Thiết bị cá nhân kết nối mạng Nhà trường phải đáp ứng yêu cầu an toàn tối thiểu; Nhà trường có quyền hạn chế hoặc ngắt kết nối thiết bị có dấu hiệu gây mất an toàn.

3. Việc sử dụng USB, ổ cứng di động và thiết bị lưu trữ ngoài đối với dữ liệu quan trọng phải thận trọng, được quét mã độc và tuân thủ quy định bảo vệ dữ liệu.

4. Không tự ý lắp bộ phát Wi-Fi, switch, camera, thiết bị IoT hoặc thiết bị mạng khác vào hạ tầng Nhà trường khi chưa được bộ phận công nghệ thông tin chấp thuận.

Điều 11. Bảo trì, giám sát và nhật ký hệ thống

1. Bộ phận công nghệ thông tin xây dựng kế hoạch bảo trì định kỳ; thông báo trước khi hoạt động bảo trì có khả năng gây gián đoạn dịch vụ, trừ trường hợp khẩn cấp.

2. Hệ thống quan trọng phải được theo dõi tình trạng hoạt động, dung lượng, cảnh báo và các dấu hiệu bất thường phù hợp khả năng kỹ thuật.

3. Nhật ký hệ thống, nhật ký truy cập và nhật ký xử lý sự cố được lưu giữ trong thời hạn phù hợp với mục đích vận hành, yêu cầu pháp luật và khả năng hệ thống; được bảo vệ khỏi sửa đổi, xóa trái phép.

4. Không chỉnh sửa hoặc xóa nhật ký nhằm che giấu hành vi, sự cố hoặc vi phạm.

Chương IV

BẢO ĐẢM AN TOÀN, AN NINH MẠNG VÀ DỮ LIỆU

Điều 12. Phân loại và bảo vệ hệ thống, thông tin

1. Nhà trường rà soát, phân loại hệ thống và thông tin theo tính chất, phạm vi sử dụng, mức độ quan trọng và rủi ro; thực hiện các yêu cầu về xác định cấp độ, bảo đảm an ninh mạng theo quy định pháp luật khi thuộc đối tượng áp dụng.

2. Dữ liệu cá nhân, dữ liệu nhân sự, tài chính, hồ sơ học sinh, kết quả học tập, dữ liệu sức khỏe, dữ liệu camera và thông tin nội bộ phải được bảo vệ theo tính chất và mức độ nhạy cảm.

3. Dữ liệu quan trọng phải được bảo vệ trong quá trình lưu trữ và truyền tải bằng biện pháp phù hợp; ưu tiên mã hóa, kiểm soát truy cập và tách biệt môi trường khi khả thi.

4. Việc xử lý dữ liệu cá nhân thực hiện theo Quy chế quản lý cơ sở dữ liệu và bảo vệ dữ liệu cá nhân của Nhà trường và pháp luật hiện hành.

Điều 13. Phòng chống mã độc, lừa đảo và tấn công mạng

1. Thiết bị do Nhà trường quản lý phải có giải pháp phòng chống mã độc phù hợp và được cập nhật thường xuyên.

2. Người dùng không mở liên kết, tệp đính kèm đáng ngờ; không cung cấp mật khẩu, mã OTP hoặc thông tin xác thực qua thư, tin nhắn, cuộc gọi không xác minh.

3. Bộ phận công nghệ thông tin được áp dụng biện pháp chặn địa chỉ, tên miền, tệp, thiết bị hoặc kết nối có dấu hiệu độc hại; cô lập thiết bị nghi nhiễm để kiểm tra.

4. Khi phát hiện chiến dịch lừa đảo hoặc nguy cơ ảnh hưởng nhiều người dùng, Nhà trường thông tin cảnh báo kịp thời.

Điều 14. Sao lưu và phục hồi dữ liệu

1. Dữ liệu và cấu hình quan trọng phải được sao lưu định kỳ theo mức độ quan trọng và khả năng thay đổi của dữ liệu.

2. Bản sao lưu quan trọng phải có ít nhất một bản tách biệt hợp lý với hệ thống vận hành chính; áp dụng kiểm soát truy cập và mã hóa khi phù hợp.

3. Định kỳ kiểm tra khả năng khôi phục; kết quả kiểm tra phải được ghi nhận. Sao lưu chỉ được coi là hiệu quả khi có khả năng phục hồi dữ liệu cần thiết.

4. Việc phục hồi dữ liệu phải bảo đảm đúng thẩm quyền, hạn chế ghi đè hoặc làm mất chứng cứ khi sự cố có dấu hiệu tấn công mạng.

Điều 15. Bảo vệ hạ tầng vật lý

1. Phòng máy chủ, tủ mạng, thiết bị lưu trữ và khu vực kỹ thuật quan trọng phải được kiểm soát người ra vào, bảo đảm nguồn điện, nhiệt độ, phòng cháy chữa cháy và điều kiện môi trường phù hợp.

2. Chỉ nhân sự được phân công hoặc người được phép mới được tiếp cận thiết bị trọng yếu; khách, nhà thầu phải có người phụ trách phối hợp khi làm việc tại khu vực kỹ thuật.

3. Không để thông tin tài khoản, sơ đồ mạng, mật khẩu hoặc tài liệu kỹ thuật nhạy cảm tại nơi người không có trách nhiệm có thể tiếp cận.

Điều 16. Dịch vụ đám mây, nhà cung cấp và bên thứ ba

1. Việc thuê, sử dụng dịch vụ đám mây, phần mềm, lưu trữ, đường truyền hoặc dịch vụ kỹ thuật phải xem xét yêu cầu về bảo mật, dữ liệu cá nhân, sao lưu, quyền truy cập, vị trí/lưu chuyển dữ liệu khi có liên quan và khả năng bàn giao dữ liệu khi chấm dứt dịch vụ.

2. Nhà cung cấp chỉ được truy cập hệ thống, dữ liệu trong phạm vi cần thiết và thời gian được cho phép; tài khoản hỗ trợ kỹ thuật phải được quản lý, thu hồi sau khi hoàn thành khi không còn nhu cầu.

3. Hợp đồng hoặc thỏa thuận có liên quan đến dữ liệu và hệ thống quan trọng cần quy định trách nhiệm bảo mật, thông báo sự cố, hoàn trả/xóa dữ liệu và phối hợp xử lý khi chấm dứt dịch vụ.

Điều 17. Sử dụng công cụ trí tuệ nhân tạo và dịch vụ trực tuyến

1. Không nhập lên công cụ trí tuệ nhân tạo công cộng hoặc dịch vụ trực tuyến chưa được Nhà trường cho phép các mật khẩu, khóa truy cập, dữ liệu cá nhân nhạy cảm, dữ liệu học sinh có khả năng định danh, hồ sơ nhân sự, tài chính, đề kiểm tra chưa công bố, cấu hình bảo mật hoặc thông tin nội bộ cần bảo vệ.

2. Khi sử dụng công cụ AI phục vụ công việc, người dùng phải kiểm tra nội dung đầu ra, bảo đảm bản quyền, tính chính xác và không để công cụ thay thế trách nhiệm chuyên môn, trách nhiệm phê duyệt của cá nhân.

3. Bộ phận công nghệ thông tin phối hợp các đơn vị hướng dẫn danh mục, cách thức sử dụng công cụ số, AI phù hợp với yêu cầu an toàn thông tin và bảo vệ dữ liệu.

Chương V ỨNG PHÓ VÀ XỬ LÝ SỰ CỐ

Điều 18. Tiếp nhận, phân loại và xử lý sự cố

1. Mọi người dùng có trách nhiệm báo ngay sự cố hoặc dấu hiệu bất thường cho bộ phận công nghệ thông tin; không tự ý xóa dữ liệu, cài lại máy hoặc xử lý làm mất dấu vết khi nghi ngờ bị tấn công.

2. Bộ phận công nghệ thông tin tiếp nhận, ghi nhận thời gian, hệ thống bị ảnh hưởng, mức độ tác động; thực hiện cô lập, ngăn chặn, khắc phục, phục hồi và theo dõi sau sự cố.

3. Sự cố có nguy cơ ảnh hưởng lớn đến hoạt động Nhà trường, dữ liệu cá nhân hoặc nhiều hệ thống phải được báo cáo ngay Ban Giám hiệu để chỉ đạo và thực hiện nghĩa vụ thông báo, báo cáo cơ quan có thẩm quyền khi pháp luật yêu cầu.

4. Sau sự cố nghiêm trọng phải tổ chức đánh giá nguyên nhân, phạm vi ảnh hưởng, biện pháp đã thực hiện và bài học phòng ngừa; cập nhật quy trình, cấu hình hoặc biện pháp bảo vệ khi cần thiết.

Điều 19. Bảo toàn thông tin, chứng cứ và phối hợp

1. Nhật ký, tệp tin, thiết bị và dữ liệu có liên quan đến sự cố phải được bảo toàn trong phạm vi cần thiết, hạn chế thay đổi làm ảnh hưởng việc xác minh.
2. Việc cung cấp thông tin, nhật ký hoặc dữ liệu cho cơ quan chức năng thực hiện theo thẩm quyền và quy định pháp luật.
3. Người không được phân công không tự ý phát ngôn, công bố nguyên nhân, dữ liệu bị ảnh hưởng hoặc thông tin kỹ thuật của sự cố ra bên ngoài.

Chương VI

QUẢN LÝ THIẾT BỊ CÔNG NGHỆ THÔNG TIN

Điều 20. Quản lý tài sản, cấp phát và thu hồi

1. Thiết bị công nghệ thông tin do Nhà trường trang bị phải được quản lý theo danh mục, mã tài sản hoặc phương thức theo dõi phù hợp; xác định người/bộ phận sử dụng, vị trí và tình trạng.
2. Việc mua sắm, cấp phát, điều chuyển, thu hồi, sửa chữa và thanh lý thực hiện theo quy trình quản lý tài sản và phân cấp phê duyệt của Nhà trường.
3. Khi thu hồi, điều chuyển hoặc thanh lý thiết bị lưu trữ dữ liệu, bộ phận công nghệ thông tin phải kiểm tra, sao lưu dữ liệu cần thiết và xóa dữ liệu an toàn trước khi bàn giao ra ngoài phạm vi quản lý.

Điều 21. Sử dụng, bảo quản và sửa chữa thiết bị

1. Người dùng sử dụng thiết bị đúng công năng, không tự ý tháo lắp, thay đổi linh kiện, di chuyển thiết bị cố định hoặc gọi đơn vị bên ngoài sửa chữa khi chưa được chấp thuận.
2. Sự cố, hư hỏng phải được báo cho bộ phận phụ trách; việc sửa chữa có tiếp cận ổ cứng, dữ liệu hoặc cấu hình phải được kiểm soát.
3. Trường hợp mất, thất thoát hoặc hư hỏng do vi phạm quy định, cá nhân liên quan chịu trách nhiệm theo nội quy, quy định của Nhà trường và pháp luật.

Chương VII

KIỂM TRA, GIÁM SÁT VÀ TỔ CHỨC THỰC HIỆN

Điều 22. Kiểm tra, đánh giá và nâng cao nhận thức

1. Bộ phận công nghệ thông tin chủ trì, phối hợp các đơn vị định kỳ hoặc đột xuất kiểm tra việc tuân thủ Quy chế, rà soát tài khoản, quyền truy cập, bản vá, sao lưu, thiết bị và các nguy cơ an toàn thông tin.
2. Nhà trường tổ chức tuyên truyền, tập huấn phù hợp cho cán bộ, giáo viên, nhân viên và học sinh về mật khẩu, xác thực đa yếu tố, lừa đảo trực tuyến, bảo vệ dữ liệu cá nhân, sử dụng AI an toàn và ứng phó sự cố.
3. Kết quả kiểm tra là cơ sở để chấn chỉnh, khắc phục rủi ro và cải tiến hệ thống; việc kiểm tra không được làm ảnh hưởng không cần thiết đến quyền riêng tư và hoạt động bình thường của người dùng.

Điều 23. Xử lý vi phạm

1. Tổ chức, cá nhân vi phạm Quy chế, tùy tính chất, mức độ và hậu quả, bị nhắc nhở, yêu cầu khắc phục, xem xét trách nhiệm theo nội quy/quy định của Nhà trường, bồi thường thiệt hại nếu có căn cứ hoặc chuyển cơ quan có thẩm quyền xử lý theo pháp luật.

2. Không quy định hoặc áp dụng hình thức kỷ luật, xử phạt trái thẩm quyền; việc xử lý người lao động và học sinh phải tuân thủ pháp luật và quy định chuyên ngành tương ứng.

Điều 24. Tổ chức thực hiện và hiệu lực

1. Các đơn vị, cán bộ quản lý, giáo viên, nhân viên, học sinh và tổ chức, cá nhân có liên quan chịu trách nhiệm thực hiện Quy chế này.

2. Bộ phận công nghệ thông tin chủ trì theo dõi, tổng hợp khó khăn, vướng mắc; phối hợp Phòng Tổ chức - Hành chính và Pháp chế và các đơn vị liên quan tham mưu Ban Giám hiệu sửa đổi, bổ sung khi có thay đổi pháp luật, công nghệ hoặc yêu cầu quản lý.

3. Quy chế có hiệu lực kể từ ngày Quyết định ban hành có hiệu lực. Các quy định trước đây của Nhà trường trái với Quy chế này hết hiệu lực kể từ thời điểm đó./.