UBND PHƯỜNG THỦ DẦU MỘT
TRƯỜNG TIỂU HỌC LÊ HỒNG PHONG

Số: 107a /QĐ-THLHP

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

Thủ Dầu Một, ngày 04 tháng 9 năm 2025

QUYẾT ĐỊNH
Ban hành quy chế vận hành, quản trị hệ thống mạng, an toàn thông tin năm học 2025 - 2026

Căn cứ Luật công nghệ thông tin ngày 29 tháng 6 năm 2006;

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

Căn vứ Nghị định số 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động cơ quan nhà nước;

Căn cứ Nghị định số 47/2020/NĐ-CP ngày 09 tháng 4 năm 2020 của Chính phủ về quản lý, kết nối và chia sẻ dữ liệu số của cơ quan nhà nước;

Căn cứ Quyết định số 1411/QĐ-UBND ngày 27 tháng 4 năm 2022 của Ủy ban nhân dân Thành phố ban hành kế hoạch tăng cường ứng dụng công nghệ thông tin và chuyển đổi số ngành Giáo dục và Đào tạo Thành phố Hồ Chí Minh giai đoạn 2022-2025, định hướng đến năm 2030;

Căn cứ Thông tư số 28/2020/TT-BGDĐT ngày 04 tháng 09 năm 2020 của Bộ trưởng Bộ giáo dục và Đào tạo ban hành điều lệ trường Điều lệ trường Tiểu học;

Căn cứ Quyết định số 4418/QĐ-UBND ngày 04 tháng 10 năm 2024 của Ủy ban nhân dân Thành phố Hồ Chí Minh ban hành Bộ tiêu chuẩn công nhận Trường học số trên địa bàn Thành phố Hồ Chí Minh;

Căn cứ Quyết định số 23/QĐ-UBND ngày 01/7/2025 của UBND phường Thủ Dầu Một về việc thành lập trường tiểu học Lê Hồng Phong thuộc UBND phường Thủ Dầu Một trên cơ sở tổ chức lại các đơn vị sự nghiệp công lập khi thực hiện mô hình chính quyền địa phương 02 cấp,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế vận hành, quản trị hệ thống mạng, an toàn thông tin của Trường Tiểu học Lê Hồng Phong.

Điều 2. Toàn thể cán bộ quản lý, giáo viên, nhân viên trường Tiểu học Lê Hồng Phong chịu trách nhiệm thi hành quyết định này. Quy chế này có hiệu lực thi hành kể từ năm học 2025 - 2026.

Điều 3. Các tổ chức, cá nhân liên quan chịu trách nhiệm thi hành quyết định này kể từ ngày ký./.

Nơi nhận:
- Như điều 3;
- Lưu VT.

HIỆU TRƯỞNG

Vũ Thị Hồng

QUY CHẾ VẬN HÀNH, QUẢN TRỊ HỆ THỐNG MẠNG, AN TOÀN THÔNG TIN

(Ban hành kèm theo Quyết định số 107a/QĐ-THLHP ngày 04 tháng 9 năm 2025 của Hiệu trưởng trường Tiểu học Lê Hồng Phong)

CHƯƠNG I
NHỮNG QUY ĐỊNH CHUNG

Điều 1. Phạm vi và đối tượng áp dụng

1. Quy chế này quy định về việc vận hành, quản trị hệ thống mạng, an toàn thông tin từ năm học 2025 - 2026

2. Đối tượng áp dụng bao gồm cán bộ quản lý, giáo viên, nhân viên, phụ huynh trường Tiểu học Lê Hồng Phong.

Điều 2. Trách nhiệm của thành viên khi tham gia vận hành, quản trị hệ thống mạng, an toàn thông tin

1. Các thành viên tham gia vận hành, quản trị hệ thống mạng, an toàn thông tin có trách nhiệm bảo mật tài khoản sử dụng, không để người khác làm thay công việc của mình.

2. Thực hiện đúng các quy định của pháp luật về an ninh, an toàn thông tin mạng.

Điều 3. Nguyên tắc vận hành, quản trị hệ thống mạng, an toàn thông tin

1. Bảo đảm tính đầy đủ, chính xác, kịp thời, thuận tiện cho khai thác, sử dụng, phục vụ công tác quản lý về giáo dục; đáp ứng yêu cầu, nhiệm vụ chuyển đổi số trong giáo dục và đào tạo.

2. Cán bộ quản lý, giáo viên, nhân viên, phụ huynh học sinh, các tổ chức, cá nhân có liên quan khai thác và vận hành, quản trị hệ thống mạng, an toàn thông tin dữ liệu phải được sự đồng ý của Hiệu trưởng và phải thực hiện việc khai thác và sử dụng dữ liệu theo đúng mục đích, nội dung đã được cho phép và theo quy định của pháp luật hiện hành.

3. Đảm bảo đúng, đủ các quy định về quản lý học sinh, quản lý chất lượng giáo dục học sinh, phối hợp giáo dục học sinh theo Điều lệ trường tiểu học.

4. Đảm bảo tính liên thông, kết nối, đồng bộ dữ liệu thông tin giữa các hồ sơ, sổ sách điện tử.

5. Đảm bảo đúng, đầy đủ các quy định về chuyển, báo cáo và lưu trữ thông tin

CHƯƠNG II
QUẢN TRỊ HỆ THỐNG MẠNG

Điều 4. Quản lý hạ tầng mạng

1. Các thiết bị mạng phải được đổi mật khẩu mặc định ngay khi cài đặt.
2. Cấu hình phân quyền truy cập theo cấp độ (Admin, Read-only)
3. Không cho phép truy cập qua Telnet, chỉ dùng SSH.
4. Cấu hình kiểm soát truy cập theo địa chỉ IP.
5. Thiết bị mạng phải được kiểm tra, cập nhật firmware định kỳ.
6. Mỗi thiết bị phải có nhật ký cấu hình, nhật ký thay đổi (log)

Điều 5. Quản trị máy chủ và dịch vụ

1. Máy chủ được phân quyền truy cập theo vai trò.
2. Các dịch vụ (web, mail, database…) phải được giám sát 24/7.
3. Hệ thống có cơ chế sao lưu và khôi phục định kỳ.
4. Các lỗi hệ điều hành và phần mềm phải được cập nhật kịp thời.
5. Cập nhật bảo mật cho hệ điều hành ít nhất 1 lần/tháng hoặc ngay khi có lỗi nghiêm trọng được công bố.

Điều 6. Tài khoản và truy cập

1. Mỗi người dùng có tài khoản riêng, không dùng chung.
2. Tài khoản phải có chính sách mật khẩu mạnh (ít nhất 8 ký tự, có chữ hoa, thường, số, ký tự đặc biệt)
3. Tài khoản không sử dụng sau 30 ngày phải tạm khóa hoặc thu hồi.
4. Quy trình cấp, thu hồi tài khoản phải rõ ràng, có sự phê duyệt.

CHƯƠNG III
AN TOÀN THÔNG TIN

Điều 7. Chính sách an toàn thông tin nội bộ

1. Cấm sao chép thông tin nội bộ ra thiết bị cá nhân nếu không được cấp phép.
2. Toàn bộ thiết bị làm việc phải được đăng ký và gắn mã tài sản.
3. Nhân viên vi phạm quy định an toàn thông tin sẽ bị xử lý từ nhắc nhở đến kỷ luật (tùy mức độ).
4. Tất cả người dùng đều phải cam kết tuân thủ an toàn thông tin.
5. Tổ chức định kỳ tổ chức tập huấn, kiểm tra an toàn thông tin.

Điều 8. Kiểm soát truy cập

1. Ghi nhận nhật ký truy cập, lưu trữ tối thiểu 6 tháng.
2. Áp dụng xác thực đa yếu tố (MFA) cho các hệ thống quan trọng.

Điều 9. Quản lý rủi ro và sự cố an toàn thông tin

1. Có quy trình phát hiện, ghi nhận, xử lý sự cố an toàn thông tin.

2. Có phân công nhân sự chịu trách nhiệm xử lý sựu cố.

3. Mọi sự cố phải được báo cáo, lưu hồ sơ và rút kinh nghiệm.

CHƯƠNG IV
TRÁCH NHIỆM CỦA CƠ QUAN, TỔ CHỨC, CÁ NHÂN

Điều 10. Trách nhiệm của Hiệu trưởng

1. Chỉ đạo triển khai quy chế, phê duyệt các quy trinhf liên quan đến vận hành, an toàn thông tin.

2. Phối hợp với các phòng ban tổ chức định kỳ, đánh giá định kỳ về an toàn thông tin.

3. Chịu trách nhiệm trước cơ quan nếu để xảy ra sự cố nghiêm trọng do thiếu kiểm soát từ cấp quản lý.

Điều 11. Trách nhiệm của nhân viên công nghệ thông tin

1. Thực hiện triển khai, vận hành, giám sát và bảo trì toàn bộ hệ thống mạng, máy chủ và dịch vụ công nghệ thông tin.

2. Định kỳ đánh giá rủi ro an toàn thông tin, lập kế hoạch kiểm tra, bảo trì hệ thống.

3. Ghi nhận, xử lý và lưu trữ hồ sơ các sự cố liên quan đến an toàn thông tin.

4. Báo cáo định kỳ và đột xuất về tình trạng hệ thống, các mối đe dọa bảo mật với lãnh đạo đơn vị.

Điều 12. Trách nhiệm của văn thư

1. Phối hợp với nhân viên công nghệ thông tin cập nhật kịp thời thông tin về nhân sự nghỉ việc, chuyển công tác để thu hồi tài khoản.

2. Quản lý hồ sơ cam kết bảo mật của nhân viên.

3. Hỗ trợ phổ biến, đào tạo nội bộ về quy chế an toàn thông tin cho cán bộ, giáo viên, nhân viên.

Điều 13. Trách nhiệm của cán bộ, giáo viên, nhân viên

1. Tuân thủ nghiêm túc các quy định về sử dụng tài khoản, mật khẩu và hệ thống công nghệ thông tin.

2. Không chia sẻ mật khẩu, không tự ý cài đặt phần mềm không rõ nguồn gốc lên máy tính làm việc.

3. Báo ngay cho nhân viên công nghệ thông tin nếu phát hiện sự cố, hành vi bất thường hoặc nghi ngờ bị tấn công.

4. Chịu trách nhiệm cá nhân nếu để xảy ra vi phạm quy định an toàn thông

tin do lỗi chủ quan.

CHƯƠNG IV
ĐIỀU KHOẢN THI HÀNH

Điều 14. Điều khoản thi hành

1. Quy chế này có hiệu lực thi hành từ ngày ký quyết định.

2. Cán bộ quản lý, giáo viên, nhân viên và các bộ phận chịu trách nhiệm thi hành quy chế này.

3. Quy chế này có thể điều chỉnh, bổ sung cho phù hợp theo từng thời điểm, khi cần thiết./.