ỦY BAN NHÂN DÂN
PHƯỜNG THỦ DẦU MỘT
TRƯỜNG TIỂU HỌC TRẦN PHÚ
Số: 64c/QĐ-THTP

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

Thủ Dầu Một, ngày 18 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

HIỆU TRƯỞNG TRƯỜNG TIỂU HỌC TRẦN PHÚ

Căn cứ Luật An ninh mạng năm 2018;

Căn cứ Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về bảo vệ dữ liệu cá nhân;

Căn cứ chức năng, quyền hạn của Hiệu trưởng được quy định tại thông tư 28/2020/TT-BGDĐT ngày 04/9/2020 của Bộ giáo dục và Đào tạo về thông tư ban hành 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 chức năng, nhiệm vụ của đơn vị.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này là Quy chế Vận hành, quản trị hệ thống mạng, an toàn thông tin của trường kể từ năm học 2025-2026 kèm theo quyết định này.

Điều 2. Tất cả cán bộ quản lý, giáo viên, nhân viên, người lao động và học sinh của trường có trách nhiệm cụ thể hóa những quy định trong quy chế này phù hợp với tình hình thực tế của nhà trường và trong việc thực hiện nhiệm vụ được giao.

Điều 3. Các cá nhân có tên tại Điều 2 chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- CBQL, GV, NV, HS
- Ban đại diện CMHS (để triển khai);
- Lưu VT.

HIỆU TRƯỞNG

TRƯỜNG TIỂU HỌC TRẦN PHÚ

Trần Vũ Phong Châu

QUY CHẾ

Vận hành, quản trị hệ thống mạng, an toàn thông tin năm học 2025 - 2026

(Ban hành Kèm theo Quyết định số 64c/QĐ-THTP ngày 18 tháng 9 năm 2025 của Trường Tiểu học Trần Phú)

Chương I
QUY ĐỊNH CHUNG

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

Quy chế này quy định về bảo đảm an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của trường Tiểu học Trần Phú.

Điều 2. Đối tượng áp dụng

Quy chế này áp dụng đối với tất cả cán bộ, giáo viên, nhân viên tham gia vận hành, khai thác các hệ thống thông tin của trường.

Điều 3. Giải thích từ ngữ

Trong Quy chế này, các từ ngữ dưới đây được hiểu như sau:

1. Mạng: là khái niệm chỉ mạng viễn thông cố định, di động, internet và mạng máy tính.

2. Tài khoản: bao gồm tên tài khoản và mật khẩu của người sử dụng.

3. Hệ thống thông tin: là tập hợp thiết bị phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin.

4. An toàn thông tin: là sự bảo vệ thông tin và hệ thống thông tin tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

5. Phần mềm độc hại: Là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hoặc toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

6. Người sử dụng: Cán bộ, công chức, viên chức, người lao động, học sinh và phụ huynh học sinh.

7. LogFile: Đây là một tập tin được tạo ra bởi một máy chủ web hoặc máy chủ proxy có chứa tất cả thông tin về các hoạt động trên máy chủ đó, như thông tin người truy cập, thời gian khách viếng thăm, địa chỉ IP …

8. Cán bộ quản trị mạng: Là cán bộ được giao phụ trách công tác đảm bảo hạ tầng, ứng dụng, cơ sở dữ liệu và an toàn, an ninh thông tin cho việc triển khai, vận hành, khai thác hệ thống CNTT tại trường.

Chương II
NỘI DUNG BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 4. Các biện pháp quản lý kỹ thuật cơ bản trong công tác bảo đảm an toàn thông tin

1. Tổ chức mô hình mạng: Cài đặt, cấu hình, tổ chức hệ thống mạng theo mô hình máy khách/máy chủ (client/server), hạn chế sử dụng mô hình mạng ngang hàng. Khi thiết lập các dịch vụ trên môi trường mạng Internet, chỉ cung cấp những chức năng thiết yếu nhất bảo đảm duy trì hoạt động của hệ thống thông tin; hạn chế sử dụng chức năng, cổng giao tiếp mạng, giao thức và các dịch vụ không cần thiết.

2. Quản lý hệ thống mạng không dây (Wireless LAN): Khi thiết lập mạng không dây, cần thiết lập các thông số an toàn và định kỳ ít nhất 3 tháng thay đổi mật khẩu truy cập nhằm tăng cường công tác bảo mật.

3. Tổ chức quản lý tài khoản: Tiến hành rà soát ít nhất 6 tháng một lần các tài khoản và định danh người dùng trong hệ thống thông tin. Hủy tài khoản, quyền truy nhập hệ thống thông tin, thu hồi lại tất cả các tài sản liên quan tới hệ thống thông tin (khóa, thẻ nhận dạng, thư mục lưu trữ,...) đối với người sử dụng không còn công tác hoặc không còn sử dụng do được cấp tài khoản mới.

4. Quản lý đăng nhập hệ thống: Các hệ thống thông tin cần giới hạn số lần đăng nhập vào hệ thống, tự động khóa tài khoản khi liên tục đăng nhập sai vượt quá số lần quy định. Tổ chức theo dõi, giám sát tất cả các phương pháp đăng nhập từ xa, nhất là các trường hợp đăng nhập vào hệ thống với mục đích quản trị. Tăng cường việc sử dụng mạng riêng ảo (VPN - Virtual Private Network) khi có nhu cầu làm việc từ xa; yêu cầu người sử dụng đặt mật khẩu với độ an toàn cao.

5. Quản lý nhật ký sự kiện (Log File): Hệ thống thông tin cần ghi nhận các sự kiện: Quá trình đăng nhập hệ thống, các thao tác cấu hình hệ thống, quá trình truy xuất hệ thống ... Thường xuyên kiểm tra, sao lưu (backup) các nhật ký sự kiện theo từng tháng để theo dõi, xác định những sự kiện đã xảy ra của hệ thống và hạn chế việc tràn nhật ký sự kiện gây ảnh hưởng đến hoạt động của hệ thống.

6. Chống phần mềm độc hại: Triển khai các phần mềm chống mã độc trên các máy tính, thiết bị di động trong mạng để phát hiện, loại trừ phần mềm độc hại. Thường xuyên cập nhật các phiên bản mới, các bản vá lỗi của các phần mềm chống virus để bảo đảm chương trình quét virus của cơ quan trên các máy chủ, máy trạm luôn được cập nhật mới nhất; thiết lập chế độ quét thường xuyên ít nhất tuần 01 lần. Thường xuyên cập nhật bản vá các lỗ hổng bảo mật của hệ điều hành

và các phần mềm ứng dụng trên máy tính để hạn chế tối đa rủi ro mất an toàn thông tin.

7. Bảo đảm an toàn cho Trang thông tin điện tử: Thực hiện theo hướng dẫn tại Công văn số 2132/BTTTT-VNCERT ngày 18/7/2011 của Bộ Thông tin và Truyền thông về việc hướng dẫn đảm bảo an toàn thông tin cho các Trang thông tin điện tử.

8. Thiết lập cơ chế sao lưu và phục hồi cho máy chủ, máy trạm: Máy chủ và máy trạm cần được thực hiện các biện pháp sao lưu dữ liệu, thông tin quan trọng nhằm phục vụ cho công tác phục hồi dữ liệu một cách nhanh nhất.

9. Xử lý khẩn cấp: Khi phát hiện hệ thống thông tin bị tấn công cần thực hiện các bước cơ bản sau:

a) Bước 1: Ngắt kết nối máy chủ ra khỏi mạng;

b) Bước 2: Sao chép nhật ký sự kiện và toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ (phục vụ cho hoạt động phân tích, điều tra);

c) Bước 3: Khôi phục hệ thống bằng cách chuyển dữ liệu sao lưu mới nhất để hệ thống hoạt động trở lại;

d) Bước 4: Chủ trì, phối hợp với các cơ quan liên quan thành lập đoàn kiểm tra an toàn thông tin định kỳ hàng năm hoặc kiểm tra đột xuất khi phát hiện có các dấu hiệu vi phạm an toàn thông tin.

Điều 5. Các biện pháp quản lý vận hành trong công tác bảo đảm an toàn thông tin

1. Đối với cán bộ chuyên trách Công nghệ thông tin (CNTT)

a) Triển khai, thực hiện các nội dung của Điều 4 Quy chế này;

b) Nắm vững và thực hiện nghiêm túc các quy định về bảo vệ bí mật Nhà nước. Thường xuyên tự cập nhật các kiến thức về an toàn thông tin, nguy cơ tiềm ẩn có thể gây mất thông tin và các biện pháp phòng tránh khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ;

c) Phối hợp chặt chẽ với cơ quan Công an trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn, an ninh thông tin.

2. Đối với người sử dụng là cán bộ, công chức, viên chức, người lao động trong nhà trường

a) Thường xuyên cập nhật những chính sách, quy trình, thủ tục an toàn thông tin của nhà trường cũng như thực hiện những hướng dẫn về an toàn thông tin của cán bộ chuyên trách công nghệ thông tin;

b) Hạn chế việc sử dụng chức năng chia sẻ tài nguyên, khi sử dụng chức năng này cần bật thuộc tính bảo mật bằng mật khẩu và thực hiện việc thu hồi chức năng này khi đã sử dụng xong;

c) Các tài khoản đăng nhập hệ điều hành cần phải đặt mật khẩu, khi không sử dụng thì phải khóa tài khoản.

3. Đối với người sử dụng là phụ huynh:

a) Nắm rõ các quy định về quy trình, thủ tục an toàn thông tin của nhà trường.

b) Thiết lập và thống nhất với con các quy định cụ thể về việc sử dụng mạng Internet. Nội dung quy định có thể bao gồm:

- Lưu ý những hoạt động mạng có thể gây nguy hiểm cho con nhằm giúp con tránh gặp phải thông tin chưa kiểm duyệt và các tiếp xúc nguy hiểm ở các diễn đàn trò chuyện không được quản lý.

- Giám sát việc sử dụng của con thông qua việc kiểm tra lịch sử truy cập mạng và các trình duyệt web mà con đăng nhập trên thiết bị điện tử.

- Làm gương để con thấy ba mẹ cũng thực hiện đúng các nội dung đề ra về việc sử dụng thiết bị và hoạt động mạng trong gia đình.

c) Nhắc nhở con ý thức về nội dung và hành vi thể hiện khi hoạt động trực tuyến. Hướng dẫn con cách thu thập chứng cứ và báo cáo nội dung không phù hợp phát hiện trên mạng.

d) Dạy cho con cách bảo vệ danh tính bản thân bằng cách giới hạn thông tin cá nhân chia sẻ trên mạng, cách tạo mật khẩu mạnh cho các tài khoản và giữ bí mật các mật khẩu này.

4. Đối với người sử dụng là học sinh:

a) Nắm rõ các quy định về quy trình, thủ tục an toàn thông tin của nhà trường.

b) Ủng hộ các thông điệp tích cực trên mạng.

c) Suy nghĩ kĩ trước khi chia sẻ suy nghĩ, hình ảnh, video clips.

d) Kiểm soát thời gian sử dụng internet, đảm bảo lịch học tập và sinh hoạt của bản thân.

Chương III
QUY ĐỊNH BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 6. Bảo vệ bí mật nhà nước trong hoạt động ứng dụng công nghệ thông tin

1. Quy định về soạn thảo, in ấn, phát hành và sao chụp tài liệu mật

a) Không được sử dụng máy tính nối mạng internet để soạn thảo văn bản, chuyển giao, lưu trữ thông tin có nội dung thuộc bí mật nhà nước; cung cấp tin, tài liệu và đưa thông tin bí mật nhà nước trên Cổng/Trang thông tin điện tử;

b) Không được in, sao chụp tài liệu bí mật nhà nước trên các thiết bị kết nối mạng internet.

2. Khi sửa chữa, khắc phục các sự cố của máy tính dùng soạn thảo văn bản mật, các phòng, đơn vị phải báo cáo cho người có thẩm quyền. Không được cho phép các công ty tư nhân hoặc người không có trách nhiệm trực tiếp sửa chữa, xử lý, khắc phục sự cố;

3. Trước khi thanh lý các máy tính trong các cơ quan nhà nước, cán bộ chuyên trách công nghệ thông tin phải dùng các biện pháp kỹ thuật xoá bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính.

Điều 7. Quy định về cấp phát, thu hồi, cập nhật và quản lý các tài khoản truy cập vào hệ thống thông tin

Cán bộ quản trị mạng quản lý, cấp tài khoản cá nhân và phân quyền truy cập cho người sử dụng trên tất cả các máy trạm đặt tại các phòng, đơn vị thuộc Ban Quản lý. Trong trường hợp cần thiết có thể hủy tài khoản truy cập cá nhân và ngắt kết nối đối với các hành vi cố ý tấn công hoặc gây trở ngại cho mạng máy tính; hủy quyền truy cập hệ thống thông tin đối với cán bộ, giáo viên, nhân viên nghỉ chế độ, chuyển công tác và đảm bảo khả năng vẫn truy nhập được vào các hồ sơ được tạo ra bởi cán bộ, giáo viên, nhân viên đó.

Hướng dẫn người sử dụng thay đổi mật khẩu ngay sau khi đăng nhập lần đầu tiên; bảo vệ thông tin của tài khoản theo quy định.

Điều 8. Cơ chế sao lưu dữ liệu

1. Cán bộ quản trị mạng phối hợp với các đơn vị có liên quan thực hiện xác định các thông tin, thực hiện quy trình sao lưu dự phòng và phục hồi cho các phần mềm, dữ liệu cần thiết theo quy định, quy trình sao lưu, lưu trữ hiện có. Các nội dung thực hiện gồm: lập danh sách các dữ liệu (thông tin cấu hình của mạng, máy chủ), phần mềm ứng dụng, cơ sở dữ liệu, tệp tin ghi nhật ký hệ được sao lưu, có phân loại theo thời gian lưu trữ, thời gian sao lưu, phương pháp sao lưu và thời gian kiểm tra phục hồi hệ thống từ dữ liệu sao lưu; thực hiện quy trình sao lưu dự phòng và phục hồi.

2. Dữ liệu sao lưu phải được lưu trữ an toàn trên Hệ thống lưu trữ dự phòng, thiết bị lưu trữ ngoài và được kiểm tra thường xuyên đảm bảo sẵn sàng cho việc

sử dụng khi cần; việc kiểm tra, phục hồi hệ thống từ dữ liệu sao lưu tối thiểu 6 tháng một lần (hoặc khi có yêu cầu đột xuất).

Điều 9. Cơ chế thông tin, báo cáo và khắc phục sự cố an toàn, an ninh thông tin

1. Đối với người sử dụng

a) Thông tin, báo cáo kịp thời cho cán bộ quản trị mạng của Ban Quản lý khi phát hiện các sự cố gây mất an toàn, an ninh thông tin mạng trong quá trình tham gia vào hệ thống thông tin;

b) Phối hợp tích cực trong suốt quá trình giải quyết và khắc phục sự cố.

2. Đối với cán bộ quản trị mạng

a) Áp dụng mọi biện pháp để khắc phục và hạn chế thiệt hại do sự cố xảy ra, lập biên bản báo cáo Ban Giám hiệu trường;

b) Cung cấp đầy đủ, chính xác, kịp thời những thông tin cần thiết; thực hiện theo đúng hướng dẫn và tạo điều kiện thuận lợi cho cơ quan chức năng tham gia khắc phục sự cố.

Chương V
KHEN THƯỞNG, XỬ LÝ VI PHẠM

Điều 10. Khen thưởng

Các tổ chuyên môn; cán bộ, giáo viên, viên chức và người lao động thực hiện tốt Quy chế này sẽ được xem xét đánh giá khen thưởng.

Điều 11. Xử lý vi phạm

Các tổ chuyên môn; cán bộ, giáo viên, viên chức và người lao động có hành vi vi phạm quy chế này thì tùy theo tính chất, mức độ vi phạm bị xử lý kỷ luật. Nếu gây thiệt hại có tính chất nghiêm trọng thì phải bồi thường về vật chất và bị truy cứu trách nhiệm hình sự theo quy định của Pháp luật hiện hành.

Chương VI
TỔ CHỨC THỰC HIỆN

Điều 12. Điều khoản thi hành

Trong quá trình thực hiện Quy chế này nếu phát hiện những điều không phù hợp, vướng mắc cần sửa đổi, bổ sung, các cá nhân kịp thời báo cáo về Văn phòng để tổng hợp trình Hiệu trưởng trường xem xét, điều chỉnh, bổ sung cho phù hợp.