UBND XÃ CÁT THÀNH
TRƯỜNG MN CÁT THÀNH

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

Số: 27/QĐ-MNCT

Cát Thành, ngày 27 tháng 10 năm 2025

QUYẾT ĐỊNH
BAN HÀNH QUY CHẾ BẢO ĐẢM AN TOÀN, AN NINH THÔNG TIN MẠNG TRƯỜNG MẦM NON CÁT THÀNH NĂM HỌC 2025-2026
HIỆU TRƯỞNG TRƯỜNG MẦM NON CÁT THÀNH

- Căn cứ Luật An ninh mạng số 24/2018/QH14.

- Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13.

- Căn cứ Chỉ thị số 14/CT-TTg ngày 7/6/2019 của Thủ tướng Chính phủ về tăng cường bảo đảm an toàn, an ninh mạng.

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

- Xét đề nghị của viên chức phụ trách công nghệ thông tin của trường Mầm non Cát Thành.

QUYẾT ĐỊNH

- Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn, an ninh thông tin mạng nội bộ của Trường Mầm non cát Thành.

- Điều 2. Quyết định này có hiệu lực từ ngày ký.

- Điều 3. Lãnh đạo trường, viên chức được giao phụ trách công nghệ thông tin của phòng chịu trách nhiệm thi hành Quyết định này.

HIỆU TRƯỞNG

U.B.N.D XÃ CÁT THÀNH T. NINH BÌNH
TRƯỜNG MẦM NON CÁT THÀNH

Phạm Thị Mận

QUY CHẾ

Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống Mạng nội bộ
(Kèm theo Quyết định số 27/QĐ-MNCT, ngày 27/10/2025 của trường mầm non Cát Thành)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh:

Quy chế này quy định các chính sách quản lý và các biện pháp nhằm bảo đảm an toàn

thông tin cho Hệ thống Mạng nội bộ của Trường Mầm non Cát Thành bao gồm:

- Phạm vi quản lý về vật lý và logic của tổ chức;
- Các ứng dụng, dịch vụ hệ thống cung cấp;
- Nguồn nhân lực bảo đảm an toàn thông tin.

2. Đối tượng áp dụng:

a) Tất cả cán bộ quản lý, giáo viên và nhân viên trường Mầm non Cát Thành.

b) Cơ quan, tổ chức, cá nhân có kết nối, sử dụng hệ thống.

c) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ quản lý, vận hành, duy trì, phát triển

và bảo đảm an toàn thông tin mạng phục vụ hoạt động của Hệ thống Mạng nội bộ.

II. Điều 2:

1. An toàn thông tin: bao gồm các hoạt động quản lý, nghiệp vụ và kỹ thuật đối với hệ thống thông tin nhằm bảo vệ, khôi phục các hệ thống, các dịch vụ và nội dung thông tin đối với nguy cơ tự nhiên hoặc do con người gây ra. An toàn thông tin bao hàm các nội dung bảo vệ và bảo mật thông tin, an toàn dữ liệu, an toàn máy tính và an toàn mạng.

2. Hệ thống thông tin: là một hệ thống bao gồm con người, dữ liệu, các quy trình và công nghệ thông tin tương tác với nhau để thu thập, xử lý, lưu trữ và cung cấp thông tin cần thiết nhằm hỗ trợ cho một hệ thống.

3. Tính toàn vẹn: bảo vệ tính chính xác và tính đầy đủ của thông tin và các phương pháp xử lý thông tin.

4. Tính tin cậy: đảm bảo thông tin chỉ có thể được truy cập bởi những người được cấp quyền sử dụng.

5. Tính sẵn sàng: đảm bảo những người được cấp quyền có thể truy cập thông tin và các tài nguyên (mạng, máy chủ, tên miền, tài khoản thư điện tử,...) ngay khi có nhu cầu.

6. Người dùng: CBGVNV của Trường Mầm non Cát Thành sử dụng máy tính, các thiết bị điện tử để xử lý công việc.

7. Tham số mạng: Là các tham số kỹ thuật được cài đặt trong các thiết bị mạng và thiết bị máy tính để tạo ra các địa chỉ kết nối trong mạng. Các máy tính gửi và nhận thông tin thông qua các địa chỉ kết nối này.

III. Điều 3. Mục tiêu, nguyên tắc bảo đảm an toàn thông tin

1. Mục tiêu bảo đảm an toàn thông tin

Bảo vệ thông tin, hệ thống thông tin trên mạng 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 Hệ thống của nhà trường.

2. Nguyên tắc

a) Cơ quan, tổ chức, cá nhân thuộc đối tượng áp dụng Quy chế này có trách nhiệm bảo đảm an toàn thông tin và hệ thống thông tin trong phạm vi xử lý công việc của mình theo quy định của pháp luật, hướng dẫn của cơ quan, đơn vị có thẩm quyền và các quy định

tại Quy chế này.

b) Bảo đảm an toàn thông tin (ATTT) là yêu cầu bắt buộc, phải được thực hiện thường xuyên, liên tục trong quá trình:Thu thập, tạo lập, xử lý, truyền tải, lưu trữ và sử dụng thông tin, dữ liệu. Thiết kế, thiết lập và vận hành, nâng cấp, hủy bỏ hệ thống thông tin.

c) Việc bảo đảm an toàn Hệ thống Mạng nội bộ được thực hiện một cách tổng thể, đồng bộ, tập trung trong việc đầu tư các giải pháp bảo vệ, có sự dùng chung, chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư thừa, trùng lặp.

IV. Điều 4. Những hành vi nghiêm cấm:

-Các hành vi bị nghiêm cấm quy định tại Điều 7 Luật An toàn thông tin mạng và

Điều 8 Luật An ninh mạng. Điều 5. Quy định chung về bảo đảm an toàn thông tin

1. Quản lý an toàn mạng:

a) Hệ thống mạng nội bộ (Mạng LAN) được thiết kế thống nhất, được quản lý định

danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý và bảo đảm an toàn và bảo mật.

b) Mạng LAN phải được bảo vệ bằng tường lửa và phân chia hệ thống mạng thành 03

vùng mạng quản lý theo chính sách an toàn thông tin riêng (vùng mạng biên, vùng mạng

nội bộ, vùng mạng không dây).

c) Vùng Mạng không dây (Wifi), 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. Hệ thống mạng

không dây phải được bảo vệ bởi mật khẩu an toàn.

2. Tất cả CBGVNV phải thực hiện tốt các công việc sau:

a) Thường xuyên quét virus trước khi đọc hoặc sao chép dữ liệu trên các thiết bị lưu

trữ ngoài như: ổ cứng di động, các loại thẻ nhớ, thiết bị lưu trữ USB,....

b) Không sử dụng các máy tính thuộc sở hữu cá nhân (máy xách tay của cá nhân, PDA) hoặc những thiết bị lưu trữ di động cá nhân chứa các dữ liệu quan trọng của cơ quan. Hạn chế tối đa việc sử dụng các thiết bị lưu trữ ngoài để sao chép, di chuyển dữ liệu.

c) Các thiết bị đầu cuối khi kết nối vào Mạng LAN phải được quản lý và cập nhật thông tin (tên, chủng loại, địa chỉ MAC, địa chỉ IP). Cần sử dụng cơ chế xác thực và sửdụng giao thức mạng an toàn.

d) Phải có trách nhiệm đảm bảo ATTT đối với từng vị trí công việc. Trước khi tham gia vào hệ thống phải được kiểm tra khả năng đáp ứng các yêu cầu về ATTT. Tuân thủ các

quy định về ATTT, nhằm đảm bảo ATTT cho hệ thống. Phải có trách nhiệm tự quản lý,

bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp thiết bị.

e) Cán bộ, công chức chấm dứt hoặc thay đổi công việc phải thu hồi tài khoản truy cập,

thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của Phòng Giáo dục và Đào tạo .

f) Phối hợp với những cơ quan/tổ chức có thẩm quyền: Phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin: Tùy theo mức độ sự cố, phối hợp với Sở Thông tin và Truyền thông, Đội Ứng cứu sự cố an toàn thông tin mạng của tỉnh để được hướng dẫn xử lý, ứng cứu các sự cố an toàn thông tin mạng.

Chương II

BẢO ĐẢM AN TOÀN THÔNG TIN TRONG QUẢN LÝ THIẾT KẾ, XÂY DỰNG HỆ THỐNG

Điều 6. Thiết kế an toàn hệ thống thông tin

1. Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận

hành hệ thống thông tin.

2. Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin.

Điều 7. Thử nghiệm và nghiệm thu hệ thống

Thực hiện thử nghiệm và nghiệm thu hệ thống trước khi bàn giao và đưa vào sử dụng

theo quy định của pháp luật:

- Đơn vị triển khai xây dựng kế hoạch, nội dung thử nghiệm hệ thống, trình cấp có

thẩm quyền phê duyệt, trước khi thực hiện thử nghiệm và nghiệm thu hệ thống.

- Hệ thống phải được thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai

thác sử dụng theo nội dung, kế hoạch được phê duyệt.

Chương III

BẢO ĐẢM AN TOÀN THÔNG TIN TRONG QUẢN LÝ VẬN HÀNH HỆ THỐNG

Điều 8. Quản lý an toàn mạng

1. Quản lý, vận hành hoạt động bình thường của hệ thống:

a) Bảo đảm cho hệ điều hành, phần mềm cài đặt trên máy chủ hoạt động liên tục, ổn

định và an toàn.

b) Thường xuyên kiểm tra cấu hình, các file nhật ký hoạt động của hệ điều hành, phần

mềm nhằm kịp thời phát hiện và xử lý những sự cố nếu có.

c) Quản lý các thay đổi cấu hình kỹ thuật của hệ điều hành, phần mềm.

d) Thường xuyên cập nhật các bản vá lỗi hệ điều hành, phần mềm từ nhà cung cấp.

đ) Loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không

còn nhu cầu sử dụng.

e) Các bản quyền phần mềm cần được thống kê, quản lý thời gian hạn phục vụ cho

việc gia hạn.

2. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố:

Triển khai hệ thống/phương tiện lưu trữ nhật ký độc lập và phù hợp với hoạt động

của các thiết bị mạng. Dữ liệu nhật ký phải được lưu tối thiểu 06 tháng.

3. Truy cập và quản lý cấu hình hệ thống:

a) Cán bộ quản lý, nhân viên vận hành truy cập, khai thác thông tin tại

hệ thống theo trách nhiệm và phân quyền được quy định; việc khai thác thông tin phải bảo đảm nguyên tắc bảo mật, không được tự ý cung cấp thông tin ra bên ngoài.

b) Cán bộ quản lý, nhân viên vận hành có trách nhiệm theo dõi và phát hiện các trường

hợp truy cập hệ thống trái phép hoặc thao tác vượt quá giới hạn, báo cáo cho cán bộ quản

lý để tiến hành ngăn chặn, thu hồi, khóa quyền truy cập của các tài khoản vi phạm.

c) Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống (cứng hóa) trước khi đưa vào vận hành, khai thác.

Điều 9. Quản lý an toàn ứng dụng:

1. Các yêu cầu, thiết kế về an toàn bảo mật của phần mềm ứng dụng cần được xác định rõ trong tài liệu phân tích, thiết kế. Trong quá trình triển khai, vận hành các

phần mềm ứng dụng cần đảm bảo nghiêm ngặt theo các yêu cầu, thiết kế về an toàn bảo mật theo quy định.

2. Ứng dụng phải được thiết lập chính sách xác thực; Kiểm soát truy cập; nhật ký hệ

thống; kết nối với hệ thống giám sát hoặc chia sẻ thông tin giám sát tập trung của tỉnh.

3. Thay đổi các tài khoản, mật khẩu mặc định ngay khi đưa phần mềm vào sử dụng.

4. Cấp quyền quản lý truy cập của người sử dụng trên phần mềm ứng dụng.

5. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố.

6. Kiểm tra, thử nghiệm và có biên bản đánh giá tính an toàn, bảo mật đối với phần

mềm ứng dụng theo quy định trước khi nghiệm. Việc tiến hành thử nghiệm phải đảm bảo

trên môi trường riêng biệt.

Điều 10. Quản lý an toàn dữ liệu:

1. Sao lưu dự phòng và khôi phục dữ liệu (tần suất sao lưu dự phòng, phương tiện lưu trữ, thời gian lưu trữ; nơi lưu trữ, phương thức lưu trữ và phương thức lấy dữ liệu ra khỏi phương tiện lưu trữ).

2. Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ

liệu, thông tin nghiệp vụ và các thông tin, dữ liệu quan trọng khác trên hệ thống (nếu có).

3. Quản lý chặt chẽ các thiết bị lưu trữ dữ liệu, nghiêm cấm việc di chuyển, thay đổi vị trí khi chưa được phép của lãnh đạo đơn vị.

4. Quản lý và phân quyền truy cập phần mềm ứng dụng và cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ của người sử dụng. Quyền truy cập phải được phân ra theo từng cấp độ tương ứng với từng nhiệm vụ của nhân viên và phải được phê duyệt từ cấp trên.

Chương IV

TỔ CHỨC BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 11. Trách nhiệm của CBGVNV

1. Trường Mầm non Thị trấn Cái Nhum phân công viên chức làm nhiệm vụ đơn vị

chuyên trách về an toàn thông tin cho Hệ thống mạng nội bộ của đơn vị.

2. Viên chức phụ trách CNTT có trách nhiệm tổ chức các nhiệm vụ được giao và

tham mưu Lãnh đạo nhà trường tổ chức thực hiện các nhiệm vụ của chủ quản hệ thống

thông tin theo quy định tại Nghị định số 85/2016/NĐ-CP của Chính phủ, Thông tư số

12/2022/TT-BTTTT của Bộ Thông tin và Truyền thông và các hướng dẫn chuyên ngành

về công tác bảo đảm an toàn thông tin.

Điều 12. Trách nhiệm của Trường Mầm non Yên Đồng.

1. Giao viên chức phụ trách CNTT làm nhiệm vụ vận hành hệ thống mạng nội bộ của đơn vị.

2. Viên chức phụ trách CNTT có trách nhiệm xây dựng và tổ chức thực thi chính sách bảo đảm an toàn thông tin cho hệ thống mạng nội bộ của đơn vị.

3. Viên chức phụ trách CNTT có trách nhiệm tham mưu Lãnh đạo nhà trường tổ chức thực hiện các nhiệm vụ của đơn vị vận hành Hệ thống mạng nội bộ theo quy định tại Nghị định số 85/2016/NĐ-CP của Chính phủ, Thông tư số 12/2022/TT-