

Số: 80/CV- MNS1ST
Về việc đề nghị thẩm định, phê duyệt hồ
sơ đề xuất cấp độ an toàn an ninh mạng

Mường Lay, ngày 24 tháng 9 năm 2025

Kính gửi: - Công an Tỉnh Điện Biên.

Căn cứ Luật an toàn thông tin mạng ngày 19/11/2015;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về
việc bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin
và Truyền thông về việc Quy định chi tiết và hướng dẫn một số điều của Nghị định
85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về việc bảo đảm an toàn hệ thống
thông tin theo cấp độ; Tiêu chuẩn Quốc gia TCVN 11930:2017 về Công nghệ thông
tin-Các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ;

Căn cứ Chỉ thị số 09/CT-TTg ngày 23/2/2024 của Chính phủ về tuân thủ quy
định pháp luật và tăng cường đảm bảo hệ thống thông tin theo cấp độ;

Căn cứ Công điện số 33/CĐ-TTg ngày 07/4/2024 của Thủ tướng Chính phủ
về tăng cường bảo đảm an toàn thông tin mạng;

Căn cứ Công văn số 3904/CV-TBATANM ngày 05/8/2025 của Tiểu ban
An toàn, An ninh mạng tỉnh Điện Biên;

Căn cứ Công văn số 2513/SGDDĐT-QL ngày 21/8/2025 của Sở Giáo dục và
Đào tạo tỉnh Điện Biên về việc quán triệt thực hiện nghiêm túc công tác bảo đảm
an ninh, an toàn thông tin trong các cơ quan, đơn vị, trường học thuộc Ngành Giáo
dục và Đào tạo;

Công văn số 643/UBND-VHXXH ngày 04 tháng 9 năm 2025 của UBND
phường Mường Lay về việc thực hiện nghiêm túc công tác bảo đảm an ninh, an
toàn thông tin trong các đơn vị trường học.

Trường Mầm non số 1 Sá Tổng đề nghị cơ quan thẩm quyền thẩm định,
phê duyệt hồ sơ đề xuất cấp độ an toàn thông tin Hệ thống mạng LAN Trường
Mầm non số 1 Sá Tổng với các nội dung sau:

Phần 1. Thông tin chung

1. Tên hệ thống thông tin: Hệ thống mạng LAN Trường Mầm non số 1 Sá
Tổng Đơn vị vận hành hệ thống thông tin: Trường Mầm non số 1 Sá Tổng

Địa chỉ: Phường Mường Lay tỉnh Điện Biên.

4. Cấp độ an toàn hệ thống thông tin đề xuất: Cấp độ 1.

Phần 2. Hồ sơ kèm theo

Hồ sơ đề xuất cấp độ 1 an toàn thông tin cho hệ thống mạng: Trường Mầm non số 1 Sá Tổng

Tài liệu thuyết minh Hồ sơ đề xuất cấp độ (bao gồm: Thông tin tổng quan về hệ thống thông tin;

Thuyết minh cấp độ đề xuất;

Thuyết minh phương án bảo đảm an toàn thông tin.

Trên đây là Công văn đề nghị thẩm định, phê duyệt hồ sơ đề xuất cấp độ an toàn an ninh mạng của Trường Mầm non số 1 Sá Tổng./.

Nơi nhận:

- Công an phường Mường Lay;
- Lưu VT, CNTT.

**HIỆU TRƯỞNG****Lò Thị Liên Dương**

Số: 78/QĐ-MNS1ST

Mường Lay, ngày 23 tháng 9 năm 2025

QUYẾT ĐỊNH

**Ban hành Quy chế bảo đảm an toàn thông tin, an ninh mạng
Hệ thống mạng nội bộ của Trường Mầm non số 1 Sá Tổng**

HIỆU TRƯỞNG TRƯỜNG MẦM NON SỐ 1 SÁ TỔNG

Căn cứ Luật Công nghệ thông tin ngày 29/6/2006,

Căn cứ Luật an toàn thông tin mạng ngày 19/11/2015,

Căn cứ Luật an ninh mạng ngày 12/6/2016;

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

*Căn cứ Nghị định số 72/2013/NĐ-CP ngày 15/7/2013 của Chính phủ về
quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng;*

*Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về
bảo đảm an toàn hệ thống thông tin theo cấp độ;*

*Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng
Chính phủ ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm
an toàn thông tin mạng quốc gia,*

*Căn cứ Thông tư số 52/2020/TT-BGDĐT ngày 31/12/2020 của Bộ Giáo
dục và Đào tạo ban hành Điều lệ trường Mầm non;*

Theo đề nghị của cán bộ phụ trách công tác CNTT nhà trường.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn thông tin, an ninh mạng hệ thống mạng nội bộ của Trường Mầm non số 1 Sá Tổng.

Điều 2: Quyết định này có hiệu lực kể từ ngày ban hành

Điều 3: Cán bộ giáo viên, nhân viên Trường Mầm non số 1 Sá Tổng và các bộ phận có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:

- Như điều 3;
- Lưu VT.

HIỆU TRƯỞNG



Lò Thị Liên Dương

QUY CHẾ

**Bảo đảm an toàn thông tin, an ninh mạng hệ thống mạng nội bộ
của Trường Mầm non số 1 Sá Tổng**
(Kèm theo Quyết định số 78/QĐ-MNS1ST ngày 23 tháng 9 năm 2025
của Trường Mầm non số 1 Sá Tổng)

Chương I QUY ĐỊNH CHUNG

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, an ninh mạng hệ thống mạng nội bộ Trường Mầm non số 1 Sá Tổng

Phạm vi quản lý 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) Các tổ chuyên môn, tổ văn phòng, các tổ chức chính trị và cán bộ giáo viên, nhân viên, lao động hợp đồng đang làm việc thuộc Trường Mầm non số 1 Sá Tổng;

b) Cơ quan, tổ chức, cá nhân có kết nối, sử dụng Hệ thống mạng nội bộ tại Trường Mầm non số 1 Sá Tổng;

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 lan nội bộ của Trường Mầm non số 1 Sá Tổng.

Điều 2. Giải thích từ ngữ

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

1. An toàn thông tin mạng: Là sự bảo vệ thông tin, Hệ thống mạng nội bộ trên mạng tránh bị truy cập, 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.

2. Mạng: Là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua mạng viễn thông và mạng máy tính.

3. Hệ thống mạng nội bộ: Là tập hợp 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 trên mạng.

4. Chủ quản Hệ thống mạng nội bộ: Là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với Hệ thống mạng nội bộ.

5. Sự cố an toàn thông tin mạng: Là việc thông tin, Hệ thống mạng nội bộ bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.

6. Rủi ro an toàn thông tin mạng: Là những nhân tố chủ quan hoặc khách quan có khả năng ảnh hưởng tới trạng thái an toàn thông tin mạng.

7. Đánh giá rủi ro an toàn thông tin mạng: Là việc phát hiện, phân tích, ước lượng mức độ tổn hại, mối đe dọa đối với thông tin, Hệ thống mạng nội bộ.

8. Quản lý rủi ro an toàn thông tin mạng: Là việc đưa ra các biện pháp nhằm giảm thiểu rủi ro an toàn thông tin mạng.

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 mạng nội bộ 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 mạng nội bộ.

2. Nguyên tắc

a) Cơ quan, tổ chức thuộc đối tượng áp dụng Quy chế này có trách nhiệm bảo đảm an toàn thông tin và Hệ thống mạng nội bộ 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 mạng nội bộ.

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.

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. Phối hợp với những cơ quan/tổ chức có thẩm quyền

1. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin:

Hiệu trưởng nhà trường giao chuyên trách công nghệ thông tin là đầu mối liên hệ, phối hợp các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin phục vụ việc bảo đảm an toàn, an ninh mạng cho Hệ thống mạng nội bộ.

2. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin:

Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin:

* Trường Mầm non số 1 Sá Tổng.

- Người liên hệ: Bà Mào Thị Mỹ Phượng, Phó Hiệu trưởng, kiêm nhiệm phụ trách CNTT.

3. Thường xuyên tham dự các lớp diễn tập đảm bảo an toàn thông tin mạng; lớp đào tạo, tập huấn chuyên sâu về an toàn thông tin mạng khi có yêu cầu của các cơ quan, tổ chức có thẩm quyền.

Điều 6. Bảo đảm nguồn nhân lực

1. Tuyển dụng

Cán bộ được tuyển dụng vào vị trí làm về an toàn thông tin (hoặc kiêm nhiệm) có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng.

2. Trong quá trình làm việc

a) Trách nhiệm bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống:

- Với người sử dụng:

+ Người sử dụng có trách nhiệm đảm bảo ATTT đối với từng vị trí công việc.

+ Phải được thường xuyên tổ chức quán triệt các quy định về ATTT, nhằm nâng cao nhận thức về trách nhiệm đảm bảo ATTT.

+ 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.

- Với cán bộ quản lý và vận hành hệ thống mạng nội bộ

+ Cán bộ quản lý và vận hành hệ thống phải thiết lập phương pháp hạn chế truy cập mạng không dây, giám sát và điều khiển truy cập không dây, tổ chức sử dụng chứng thực và mã hóa để bảo vệ truy cập không dây tới Hệ thống mạng nội bộ.

+ Cán bộ quản lý và vận hành hệ thống phải tổ chức quản lý định danh đối với tất cả người dùng tham gia sử dụng Hệ thống mạng nội bộ.

b) Định kỳ hàng năm tổ chức hoặc tham gia phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng do đơn vị chức năng tổ chức.

3. Chấm dứt thay đổi công việc

a) Cán bộ chấm dứt hoặc thay đổi công việc phải thu hồi thẻ 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 tổ chức;

b) Bộ phận chuyên trách thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc.

Chương II

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

Điều 7. Thiết kế an toàn Hệ thống mạng nội bộ

1. Bộ phận chuyên trách xây dựng tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành Hệ thống mạng nội bộ và thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống.
2. Bộ phận chuyên trách xây dựng tài liệu mô tả thiết kế và các thành phần của Hệ thống mạng nội bộ thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống.

Điều 8. Thử nghiệm và nghiệm thu hệ thống

1. Bên triển khai xây dựng kế hoạch, nội dung thử nghiệm hệ thống trước khi thực hiện thử nghiệm và nghiệm thu hệ thống.
2. Đơn vị vận hành thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác theo phương án thiết kế được phê duyệt trong Hồ sơ đề xuất cấp độ.

Chương III

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

Điều 9. Quản lý an toàn mạng

1. Hệ thống mạng phải 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.
2. Hệ thống mạng nội bộ (LAN) phải được bảo vệ bằng tường lửa (có thể tích hợp tường lửa trên modem hoặc router) và phân chia hệ thống mạng thành các vùng mạng quản lý theo chính sách an toàn thông tin riêng.
3. Mạng không dây (WFI), 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.

Điều 10. Quản lý an toàn máy chủ và ứng dụng

1. Máy chủ phải được thiết lập chính sách xác thực và kiểm soát truy cập. Hệ thống mạng nội bộ cần có phương án giới hạn số lần đăng nhập, 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.
2. Kiểm tra, giám sát các hoạt động liên quan đến các nơi lưu trữ mật khẩu và cảnh báo khi có những hành động bất thường (Ví dụ: user không có quyền nhưng cố tình truy xuất đến các file lưu mật khẩu...).

Điều 11. Quản lý an toàn dữ liệu

1. Có cơ chế sao lưu dữ liệu dự phòng, lưu trữ dữ liệu tại nơi an toàn đồng thời thường xuyên kiểm tra để đảm bảo sẵn sàng phục hồi nhằm ngăn ngừa và hạn chế khi sự cố an toàn thông tin mạng xảy ra. Dữ liệu trên máy chủ được sao lưu thông qua hệ thống sao lưu dữ liệu.

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 theo yêu cầu của đơn vị vận hành.

3. 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.

Điều 12. Quản lý an toàn người sử dụng đầu cuối Chính sách, quy trình quản lý an toàn người sử dụng đầu cuối bao gồm:

1. Việc sử dụng các thiết bị lưu trữ ngoài như ổ cứng di động, các loại thẻ nhớ, thiết bị lưu trữ USB, ... phải thường xuyên quét virus trước khi đọc hoặc sao chép dữ liệu.

2. 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 vào mục đích khác. Hạn chế tối đa việc sử dụng các thiết bị lưu trữ ngoài để sao chép, di chuyển dữ liệu.

3. Các thiết bị đầu cuối khi kết nối 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 sử dụng giao thức mạng an toàn

4. Bộ phận chuyên trách về an toàn thông tin phải thường xuyên theo dõi, kiểm tra các lỗ hổng bảo mật và quản lý kết nối, truy cập khi sử dụng thiết bị đầu cuối từ xa, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống đối với các nhân viên đã nghỉ việc.

5. Bộ phận chuyên trách về an toàn thông tin thường xuyên theo dõi cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho máy tính người sử dụng và thực hiện quy trình trước khi đưa hệ thống vào sử dụng.

Điều 13. Quản lý rủi ro an toàn thông tin mạng

Đơn vị vận hành xây dựng và ban hành hồ sơ Quản lý rủi ro an toàn thông tin bao gồm các nội dung sau:

1. Danh mục tài sản thông tin, dữ liệu có trong hệ thống.

2. Đánh giá các rủi ro an toàn thông tin đối với mỗi loại tài sản.

3. Có phương án dự phòng và khôi phục sau sự cố đối với thông tin, dữ liệu và ứng dụng.

Điều 14. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

Cá nhân hoặc tập thể có trách nhiệm bảo đảm an toàn thông tin mạng trong quản lý, sử dụng thiết bị công nghệ thông tin được giao.

1. Quy định hủy bỏ các thông tin/dữ liệu bảo mật 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 tổ chức, cá nhân không có trách nhiệm trực tiếp sửa chữa, xử lý, khắc phục sự cố.

2. Quy định về xử lý và hủy bỏ phương tiện lưu trữ điện tử

a) Thiết bị CNTT có chứa dữ liệu (máy tính, thiết bị lưu trữ, ...) khi bị hỏng phải được cán bộ chuyên trách về công nghệ thông tin kiểm tra, sửa chữa, khắc phục.

Phải có biện pháp kiểm tra, giám sát đảm bảo không để lọt lộ thông tin hay lây nhiễm mã độc đối với máy tính mang ra bên ngoài sửa chữa, bảo hành.

b) Trước khi tiến hành thanh lý/loại bỏ thiết bị công nghệ thông tin cũ, phải áp dụng các biện pháp kỹ thuật xóa bỏ hoàn toàn dữ liệu người dùng đã tạo ra, đảm bảo không thể phục hồi.

3. Quy định về xử lý thông tin trên các phương tiện và thiết bị CNTT: Trang thiết bị công nghệ thông tin có lưu trữ dữ liệu nhạy cảm khi thay đổi mục đích sử dụng hoặc thanh lý, đơn vị phải thực hiện các biện pháp xóa, tiêu hủy dữ liệu đó đảm bảo không có khả năng phục hồi. Trường hợp không thể tiêu hủy được dữ liệu, đơn vị phải thực hiện tiêu hủy cấu phần lưu trữ dữ liệu trên trang thiết bị công nghệ thông tin đó.

Trang thiết bị công nghệ thông tin có bộ phận lưu trữ dữ liệu hoặc thiết bị lưu trữ dữ liệu khi mang bảo hành, bảo dưỡng, sửa chữa bên ngoài hoặc ngừng sử dụng phải tháo bộ phận lưu trữ khỏi thiết bị hoặc xóa thông tin, dữ liệu lưu trữ trên thiết bị (trừ trường hợp đề khôi phục dữ liệu).

4. Bộ phận chuyên trách về an toàn thông tin thường xuyên theo dõi cài đặt,

Điều 15. Trách nhiệm của nhà trường

Thực hiện trách nhiệm theo quy định tại Điều 22 Nghị định 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn Hệ thống mạng nội bộ theo cấp độ.

Điều 16. Trách nhiệm của Cán bộ và Bộ phận chuyên trách về an toàn thông tin

1. Giao cho bộ phận phụ trách Công nghệ thông tin là bộ phận chuyên trách về an toàn thông tin, có trách nhiệm bảo đảm an toàn thông tin cho hệ thống thông tin.

2. Giao cho bà Mào Thị Mỹ Phượng - Phó Hiệu trưởng (phụ trách CNTT) làm nhiệm vụ vận hành, quản lý hệ thống mạng nội bộ của đơn vị.

3. Bà Mào Thị Mỹ Phượng 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.

4. Tuân thủ các quy định về trách nhiệm của bộ phận chuyên trách an toàn thông tin và vận hành an toàn hệ thống được giao tại Quy chế này.

Điều 17. Trách nhiệm của người dùng

Thực hiện nghiêm túc các quy định về quản lý, vận hành hệ thống tại đơn vị theo đúng các quy định hiện hành. Chấp hành đúng các quy định về an toàn thông tin tại Điều 12 Quy chế này.

Chương V**TỔ CHỨC THỰC HIỆN****Điều 18. Xây dựng và công bố**

Quy chế này được tổ chức/bộ phận trình người đứng đầu đơn vị (hiệu trưởng) vận hành trước khi công bố áp dụng.

Điều 19. Rà soát, cập nhật, bổ sung Quy chế

1. Định kỳ 03 năm hoặc khi có thay đổi Quy chế bảo đảm an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung.
2. Có hồ sơ lưu lại thông tin phản hồi của đối tượng áp dụng chính sách trong quá trình triển khai, áp dụng chính sách an toàn thông tin./.