UBND PHƯỜNG MỸ LỘC
TRƯỜNG TIỂU HỌC MỸ TIÊN

Số: 11 /QĐ-THMT

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

Mỹ Lộc, ngày 07 tháng 10 năm 2025

QUYẾT ĐỊNH
Ban hành Quy chế bảo đảm an toàn hệ thống thông tin mạng nội bộ của trường Tiểu học Mỹ Tiên

HIỆU TRƯỞNG TRƯỜNG TIỂU HỌC MỸ TIÊN

Căn cứ Luật Công nghệ thông tin ngày 29 tháng 6 năm 2006; Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015; Luật An ninh mạng ngày 12 tháng 6 năm 2018;

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

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của 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 Thông tư số 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 của Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin;

Theo đề nghị của Ban Công nghệ thông tin nhà trường

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này "Quy chế bảo đảm an toàn hệ thống thông tin mạng nội bộ" của trường Tiểu học Mỹ Tiên. Quyết định này thay thế cho quyết định số 34/QĐ-THMT ngày 24/02/2025 và có hiệu lực kể từ ngày kí.

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

Điều 3. Các tổ chuyên môn, tổ văn phòng, viên chức, người lao động của trường Tiểu học Mỹ Tiên chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như điều 3;
- Đăng trang TTĐT trường;
- Lưu VT.

HIỆU TRƯỞNG

TRƯỜNG TIỂU HỌC MỸ TIÊN

Nguyễn Thị Thanh Sen

Scanned with OKEN Scanner

UBND PHƯỜNG MỸ LỘC
TRƯỜNG TIỂU HỌC MỸ TIẾN

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

QUY CHẾ
BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN MẠNG NỘI BỘ CỦA TRƯỜNG TIỂU HỌC MỸ TIẾN

(Ban hành kèm theo Quyết định số 317 QĐ-THMT ngày 07/10/2025 của Hiệu trưởng trường Tiểu học Mỹ Tiến)

CHƯƠNG I
NHỮNG QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh, đối tượng áp dụng:

1. Phạm vi điều chỉnh:

Quy chế này quy định về bảo đảm an toàn hệ thống thông tin Mạng máy tính, mạng nội bộ, Email công vụ. Áp dụng cho hệ thống mạng của trường Tiểu học Mỹ Tiến.

2. Đối tượng áp dụng:

Quy chế này áp dụng đối với viên chức và người lao động công tác tại trường Tiểu học Mỹ Tiến trong việc quản lý, sử dụng hệ thống mạng nội bộ (LAN), mạng Internet, Hệ thống Email công vụ của nhà trường.

Điều 2. Giải thích từ ngữ:

1. Thiết bị công nghệ thông tin: Là toàn bộ các trang thiết bị có liên quan đến công nghệ thông tin (CNTT) như: Máy tính (PC, Laptop, Sever), máy in, máy quét, máy chiếu, các loại ổ ghi đĩa CD, VCD, DVD, ổ cứng, thẻ nhớ (USB), camera số, máy ảnh số, thiết bị chuyển mạch (hub, switch), tường lửa (firewall), modem, hệ thống cáp mạng.

2. Tài nguyên mạng: Là toàn bộ các phần mềm dùng chung chạy trên mạng nội bộ của trường, gồm: Trang thông tin điện tử, các phần mềm dùng chung của UBND các cấp, Bộ GDĐT, Sở GDĐT, Email công vụ, các phần mềm được cài đặt trên hệ thống máy tính, các phần mềm chuyên môn, chuyên ngành...

3. Email: Là thông điệp dữ liệu được gửi đến một hoặc nhiều địa chỉ Email thông qua cơ sở hạ tầng thông tin.

4. Người sử dụng: viên chức, người lao động sử dụng các thiết bị CNTT; được cấp tài khoản (Account) gồm tên người sử dụng (Username) và mật khẩu (Password) để khai thác mạng LAN và các tài nguyên mạng nội bộ của trường thông qua mạng LAN, mạng Internet.

Scanned with OKEN Scanner

5. Quản trị mạng: Là viên chức được giao nhiệm vụ quản lý hệ thống thiết bị CNTT, duy trì sự hoạt động mạng máy tính nội bộ của nhà trường; hướng dẫn người sử dụng thiết bị CNTT và khai thác tài nguyên mạng phục vụ công tác.

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

1. Mục tiêu:

Mục tiêu bảo đảm an toàn thông tin là bảo vệ thông tin, hệ thống thông tin 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 hệ thống thông tin.

2. Nguyên tắc:

a) Hoạt động ứng dụng công nghệ thông tin thực hiện các nguyên tắc bảo đảm an toàn thông tin mạng được quy định tại Điều 4 Luật an toàn thông tin mạng năm 2015 và Điều 41 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.

b) Bảo đảm an toàn thông tin (ATTT) là yêu cầu bắt buộc, phải được thực hiện thường xuyên, liên tục, kịp thời và hiệu quả.

c) 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.

d) Việc xử lý sự cố an toàn thông tin mạng phải bảo đảm quyền và lợi ích hợp pháp của tổ chức, cá nhân, không xâm phạm đến đời sống riêng tư, bí mật cá nhân, bí mật gia đình của cá nhân, thông tin riêng của tổ chức.

3. Tài nguyên thông tin cần đảm bảo an toàn thông tin

3.1. Hệ thống hạ tầng kỹ thuật:

a) Thiết bị lưu trữ (máy chủ, máy trạm, ...).

b) Thiết bị ngoại vi (máy in, máy quét và các thiết bị số hoá, camera, thiết bị lưu trữ dữ liệu di động, ...).

c) Đường truyền dữ liệu, đường kết nối Internet.

d) Mạng nội bộ (LAN), thiết bị kết nối mạng, thiết bị bảo mật và thiết bị phụ trợ.

đ) Thiết bị công nghệ thông tin khác được kết nối mạng trong nhà trường.

3.2. Hệ thống thông tin, phần mềm, ứng dụng và cơ sở dữ liệu:

a) Hệ thống thông tin, nền tảng số, cơ sở dữ liệu dùng chung (email, quản lý văn bản và điều hành, thông tin nội bộ, quản lý nhân sự và thi đua khen thưởng, quản lý tài sản, tài chính, thư viện, hồ sơ hành chính điện tử, dữ liệu thống kê tổng hợp, ...).

b) Phần mềm, ứng dụng cung cấp dịch vụ công trực tuyến.

c) Cổng trang thông tin điện tử của trường.

d) Hệ thống thông tin nghiệp vụ và các cơ sở dữ liệu chuyên ngành.

Scanned with OKEN Scanner

d) Phần mềm, ứng dụng phục vụ công tác quản lý, điều hành hoạt động của nhà trường.

3.3. Thông tin, dữ liệu được trao đổi, truyền tải, xử lý và lưu trữ tại hệ thống thông tin của trường.

Điều 4. Nguồn nhân lực bảo đảm an toàn thông tin

1. Quy định đối với quản trị viên CNTT:

Viên chức đảm nhiệm quản trị viên CNTT an toàn thông tin cần có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin.

2. Quy định về việc thực hiện đảm bảo an toàn thông tin trong quá trình làm việc:

Trách nhiệm bảo đảm an toàn thông tin đối với người sử dụng, cán bộ quản lý và vận hành hệ thống.

a) Với người sử dụng:

- Người sử dụng 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.

- 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.

b) Với quản trị và vận hành hệ thống

- Viên chức quản lý 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 hoá để bảo vệ truy cập không dây tới hệ thống thông tin.

- Các tổ, cá nhân tham gia sử dụng các dịch vụ của hệ thống phải tuân thủ các quy định về bảo đảm an toàn, an ninh thông tin và chịu trách nhiệm đối với mọi hoạt động trên tài khoản truy cập của mình đã được cấp trên hệ thống.

3. Quy định đối với viên chức và người lao động nghỉ chế độ hoặc thay đổi công việc:

a) Khi viên chức, người lao động chấm dứt hoặc thay đổi công việc, các tài khoản truy cập hệ thống, thông tin lưu trữ trên phương tiện lưu trữ (Email công vụ) sẽ được đóng và các thiết bị, máy móc, tài sản có liên quan được phân cho người khác khác tiếp quản.

b) Quản trị hệ thống phải vô hiệu hoá tất cả các quyền ra, vào, truy cập tài khoản, quản trị hệ thống sau khi viên chức và người lao động thôi việc.

CHƯƠNG II

ĐẢM BẢO AN TOÀN THÔNG TIN TRONG THIẾT KẾ,

Scanned with OKEN Scanner

XÂY DỰNG HỆ THỐNG THÔNG TIN

Điều 5. Thiết kế, xây dựng hệ thống thông tin cần bảo đảm các yêu cầu:

1. Xây dựng tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin và thuyết minh trong hồ sơ đề xuất cấp độ của hệ thống.

2. Xây dựng tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin thuyết minh trong hồ sơ đề xuất cấp độ của hệ thống.

3. Quản trị hệ thống xây dựng tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ của hệ thống thông tin thuyết minh trong hồ sơ đề xuất cấp độ của hệ thống.

4. Ban công nghệ thông tin (CNTT) xây dựng tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin của hệ thống thông tin thuyết minh trong hồ sơ đề xuất cấp độ của hệ thống.

5. Ban CNTT trách khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống, báo cáo Lãnh đạo quyết định trước khi thực hiện thay đổi.

6. Các yêu cầu về mặt kỹ thuật để bảo đảm việc thiết kế, xây dựng và thiết lập hệ thống thông tin bảo đảm an toàn. Các yêu cầu kỹ thuật được chia thành các nhóm yêu cầu: bảo đảm an toàn mạng; bảo đảm an toàn máy chủ; bảo đảm an toàn ứng dụng; bảo đảm an toàn dữ liệu.

Điều 6. Đối với phát triển phần mềm thuê khoán cần đáp ứng:

1. Có điều khoản hợp đồng, biên bản và các cam kết đối với bên thuê khoán khi thực hiện các nội dung liên quan đến việc phát triển phần mềm thuê khoán.

2. Hiệu trưởng, quản trị CNTT có trách nhiệm quản lý và lưu trữ mã nguồn an toàn.

3. Các nhà phát triển cung cấp mã nguồn phần mềm.

a) Các nhà phát triển cung cấp mã nguồn phần mềm cho Ban CNTT.

b) Phần mềm thuê khoán phải được kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng.

c) Phần mềm thuê khoán phải được kiểm tra, đánh giá an toàn thông tin, trước khi đưa vào sử dụng.

Điều 7. Thử nghiệm và nghiệm thu hệ thống

1. Thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng;

2. Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống;

3. Ban CNTT thực hiện thử nghiệm và nghiệm thu hệ thống;

Scanned with OKEN Scanner

4. Có đơn vị độc lập (bên thứ ba) hoặc bộ phận độc lập thuộc đơn vị thực hiện tư vấn và giám sát quá trình thử nghiệm và nghiệm thu hệ thống;

5. Có báo cáo nghiệm thu được xác nhận của Ban CNTT và phê duyệt của hiệu trưởng trước khi đưa vào sử dụng.

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

Điều 8. Hệ thống Thư công vụ của trường

1. Hệ thống thư công vụ của trường là hệ thống thông tin dùng chung cung cấp dịch vụ công vụ cho nhà trường.

2. Địa chỉ thư công vụ của trường:
https://qlvbdh.ninhbinh.gov.vn/qlvbdh/main?lang=vi;
tieuhocmytien2022@gmail.com

Điều 9. Quản lý an toàn mạng

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

a) Việc bật, tắt máy tính, máy in,... phải thực theo hướng dẫn sử dụng thiết bị, hạn chế tối đa việc tắt đột ngột thiết bị.

b) Cấu hình mạng, vị trí thiết bị, quy định địa chỉ IP, tên máy trạm, máy chủ, nhóm làm việc (Workgroup), vùng làm việc (Domain) được quy định và thống nhất tại nhà trường do quản trị công nghệ thông tin thiết lập.

c) Các thông tin khi di chuyển từ ổ đĩa ngoài, USB, đĩa CD, VCD, DVD và các thư điện tử trước khi tải về phải kiểm tra, quét virus.

d) Không truy cập các trang web không biết rõ nguồn gốc. Nghiêm cấm mọi hành vi cài đặt hoặc phát tán virus vào hệ thống máy tính.

đ) Hoạt động của hệ thống phải được giám sát thường xuyên, liên tục, bảo đảm tính khả dụng của hệ thống.

e) Toàn bộ cấu hình hệ thống phải được sao lưu, dự phòng trên thiết bị hoặc hệ thống lưu trữ độc lập, định kỳ 01 tháng/lần.

g) Khi thực hiện nâng cấp, thay đổi cấu hình hệ thống phải thực hiện ngoài giờ làm việc.

h) Phải kiểm tra hoạt động tổng thể của hệ thống sau khi thay đổi cấu hình hoặc nâng cấp hệ thống.

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

a) Định kỳ hàng tháng hoặc khi có thay đổi, ban CNTT thực hiện sao lưu, dự phòng hệ thống trên hệ thống độc lập như USB, DVD hoặc SAN.

b) Các dữ liệu cần sao lưu, dự phòng: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

Scanned with OKEN Scanner

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

a) Cấu hình hệ thống từ xa phải sử dụng các giao thức bảo mật có mã hóa thông tin như SSL, TSL, SSH, VPN.

b) Khi cấu hình hệ thống từ bên ngoài phải thông qua kết nối VPN.

c) Toàn bộ cấu hình hệ thống phải được lưu trên thiết bị hoặc hệ thống lưu trữ độc lập.

d) Viên chức vận hành truy cập, khai thác thông tin 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.

đ) Hệ thống mạng phải được thiết lập cấu hình để: Kiểm soát truy cập từ bên ngoài mạng; Kiểm soát truy cập từ bên trong mạng; Kết nối về hệ thống giám sát tập trung; Phòng chống xâm nhập giữa các vùng mạng; Phòng chống phần mềm độc hại trên môi trường mạng.

e) Việc cài đặt, kết nối và gỡ bỏ thiết bị mạng trong hệ thống phải được cho phép bởi quản trị và thực hiện theo quy trình được phê duyệt.

4. Các thiết bị trong hệ thống cần được cấu hình tối ưu, tăng cường bảo mật, ưu tiên sử dụng thiết bị chuyên dụng trước khi đưa vào vận hành, khai thác.

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

1. Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ:

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) Phần mềm bản quyền cần được theo dõi quản lý thời gian sử dụng đảm bảo cho việc gia hạn đúng thời gian.

2. Truy cập mạng của máy chủ: Bảo đảm các kết nối mạng trên máy chủ hoạt động liên tục, ổn định và an toàn. Cấu hình, kiểm soát các kết nối, các cổng dịch vụ từ bên trong đi ra cũng nhưng bên ngoài vào hệ thống.

3. Truy cập và quản trị máy chủ và ứng dụng:

a) Thay đổi các tài khoản, mật khẩu mặc định ngay khi đưa hệ điều hành, phần mềm vào sử dụng.

Scanned with OKEN Scanner

b) Cấp quyền quản lý truy cập của người sử dụng trên máy chủ cài đặt hệ điều hành.

c) Toàn bộ máy chủ và thiết bị công nghệ thông tin không phải máy tính ngoại trừ các hệ thống bắt buộc phải có giao tiếp với Internet (các hệ thống phục vụ truy cập Internet; cung cấp giao diện ra Internet của trang tin điện tử; phục vụ cập nhật bản vá hệ điều hành, mẫu mã độc, mẫu điểm yếu, mẫu tấn công) không được kết nối Internet.

d) Sử dụng cơ chế xác thực đa nhân tố khi truy cập vào các máy chủ trong hệ thống, các tài khoản quản trị của ứng dụng; có cơ chế yêu cầu người sử dụng thay đổi thông tin xác thực định kỳ.

đ) Kiểm tra tính toàn vẹn của các tệp tin hệ thống và tính toàn vẹn của các quyền đã được cấp trên các tài khoản hệ thống.

e) Sử dụng cơ chế mã hóa thông tin xác thực của người sử dụng/bên sử dụng trước khi gửi đến ứng dụng qua môi trường mạng.

g) Xác thực thông tin, nguồn gửi khi trao đổi thông tin trong quá trình quản trị ứng dụng (không phải là thông tin, dữ liệu công khai) qua môi trường mạng.

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

a) Triển khai hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng.

b) Phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau thực hiện sao lưu, dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

5. Cài đặt, gỡ bỏ hệ điều hành, dịch vụ, phần mềm trên hệ thống máy chủ và ứng dụng.

6. Kết nối và gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống.

7. Cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho hệ thống máy chủ trước khi đưa vào vận hành, khai thác.

Điều 11. Quản lý an toàn dữ liệu

1. Yêu cầu an toàn đối với phương pháp mã hóa:

a) Phải áp dụng quy định sử dụng các phương thức mã hóa thích hợp theo các chuẩn quốc gia hoặc quốc tế đã được công nhận để bảo vệ thông tin.

b) Phải có biện pháp quản lý khóa mã hóa thích hợp để hỗ trợ việc sử dụng các kỹ thuật mã hóa.

2. Phân loại, quản lý và sử dụng khóa bí mật và dữ liệu mã hóa.

3. Cơ chế mã hóa và kiểm tra tính nguyên vẹn của dữ liệu.

4. Trao đổi dữ liệu qua môi trường mạng và phương tiện lưu trữ.

Scanned with OKEN Scanner

5. 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).

6. Cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ.

7. 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).

Điều 12. Quản lý an toàn thiết bị đầu cuối Quy định về quản lý an toàn thiết bị đầu cuối bao gồm các nội dung:

1. Quản lý, vận hành hoạt động bình thường cho thiết bị đầu cuối;

2. Kết nối, truy cập và sử dụng thiết bị đầu cuối từ xa;

3. Cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống;

4. 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;

5. Kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin cho thiết bị đầu cuối trước khi đưa vào sử dụng.

Điều 13. Quản lý phòng chống phần mềm độc hại

1. Tất cả máy chủ phải được trang bị phần mềm phòng chống mã độc đáp ứng yêu cầu tại Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ.

2. Khi phát hiện ra bất kỳ dấu hiện nào liên quan đến việc bị nhiễm mã độc trên máy trạm (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu, …), người sử dụng phải báo trực tiếp cho quản trị CNTT của nhà trường để xử lý.

3. Phần mềm ứng dụng trước khi được cài đặt, sử dụng phải được kiểm tra xem có phần mềm độc hại tồn tại hay không? Tất cả các tập tin, thư mục phải được quét mã độc trước khi sao chép, sử dụng.

4. Định kỳ hàng năm thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống.

Điều 14. Quản lý điểm yếu an toàn thông tin

1. Thường xuyên phổ biến, quán triệt và cập nhật những quy định về an toàn thông tin và hướng dẫn viên chức, người lao động thực hiện đúng hướng dẫn về an toàn, an ninh thông tin nhằm nâng cao nhận thức và trách nhiệm về an toàn thông tin.

2. 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 thu hồi chức năng này khi

Scanned with OKEN Scanner

đã sử dụng xong. Tuyệt đối không được tự ý kết nối thêm các máy tính, thiết bị ngoại vi (máy tính xách tay, thiết bị lưu trữ di động, bộ phát sóng wifi…) vào hệ thống mạng của nhà trường khi chưa đảm bảo điều kiện an ninh. Không được sử dụng các loại thiết bị lưu trữ ngoài để sao chép, lưu trữ các tài liệu quan trọng, đặc biệt là các thiết bị lạ, chưa được kiểm soát.

3. Các máy tính cá nhân khi không sử dụng trong thời gian dài (quá 4 giờ làm việc) cần tắt máy để tránh bị các tin tặc lợi dụng tấn công vào hệ thống thông tin của máy tính. Máy tính cá nhân phải được cài đặt phần mềm diệt virus có bản quyền.

4. Khai thác tài nguyên Internet có chọn lọc, không vào các trang web lạ, không bấm vào các đường liên kết, biểu tượng quảng cáo không rõ nội dung và không cài đặt phần mềm không rõ nguồn gốc.

5. Phải đặt mật khẩu cho máy tính (mật khẩu đăng nhập, mật khẩu bảo vệ màn hình), Sử dụng các thiết bị lưu trữ thông tin (USB, Thẻ nhớ…) đảm bảo an toàn, đúng cách để phòng ngừa vi rút, phần mềm gián điệp xâm nhập máy tính phá hoại, đánh cắp thông tin.

6. Quản lý thông tin điểm yếu an toàn thông tin đối với từng thành phần có trong hệ thống (hệ điều hành, máy chủ, ứng dụng, dịch vụ…); phân loại mức độ nguy hiểm của điểm yếu; xây dựng phương án và quy trình xử lý đối với từng mức độ nguy hiểm của điểm yếu.

7. Báo cáo hiệu trưởng ngay khi phát hiện điểm yếu an toàn thông tin ở mức độ nghiêm trọng. Thực hiện cảnh báo và xử lý điểm yếu an toàn thông tin theo chỉ đạo. Việc xử lý điểm yếu an toàn thông tin phải bảo đảm không làm ảnh hưởng/gián đoạn hoạt động của hệ thống.

8. Có trách nhiệm phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu an toàn thông tin đối với các điểm yếu khi cần thiết.

9. Kiểm tra, đánh giá và xử lý điểm yếu an toàn thông tin cho thiết bị hệ thống, máy chủ, dịch vụ trước khi đưa vào sử dụng.

10. Định kỳ 1 năm kiểm tra, đánh giá điểm yếu an toàn thông tin cho toàn bộ hệ thống thông tin; Thực hiện quy trình kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin khi có thông tin hoặc nhận được cảnh báo về điểm yếu an toàn thông tin đối với thành phần cụ thể trong hệ thống.

Điều 15. Quản lý giám sát an toàn hệ thống thông tin

1. Triển khai hệ thống giám sát trung tâm phải đáp ứng yêu cầu tại khoản 1, Điều 5 Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin.

2. Thông tin giám sát và danh mục các đối tượng giám sát phải đáp ứng yêu cầu tại khoản 2, Điều 5 Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin

Scanned with OKEN Scanner

3. Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát.

4. Thực thi nhiệm vụ giám sát theo quy định tại khoản 3, Điều 5 Thông tư số 31/2017/TT-BTTTT.

Điều 16. Quản lý sự cố an toàn thông tin

1. Phân nhóm sự cố an toàn thông tin mạng theo quy định tại Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ ngày 16/3/2017 quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia (Quyết định 05).

2. Quyết định toàn diện về mặt kỹ thuật đối với cơ quan trong quá trình khắc phục sự cố về ATTT; Hỗ trợ, phối hợp và hướng dẫn các cơ quan khắc phục sự cố mất ATTT; Yêu cầu ngưng hoạt động một phần hoặc toàn bộ các hệ thống thông tin của các cơ quan nhằm phục vụ công tác khắc phục sự cố về ATTT; Phối hợp với đơn vị chức năng trong điều tra các nguyên nhân gây ra sự cố mất an toàn thông tin theo chỉ đạo của Lãnh đạo.

3. Ban CNTT phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin; Yêu cầu bên cung cấp, hỗ trợ cung cấp quy trình xử lý sự cố cho các dịch vụ do bên cung cấp, hỗ trợ cung cấp liên quan đến hệ thống.

Điều 17. Quản lý an toàn người sử dụng đầu cuối

1. Kết nối máy tính/thiết bị đầu cuối của người sử dụng vào hệ thống

a) Người sử dụng khi truy cập, sử dụng tài nguyên nội bộ, truy cập mạng và tài nguyên trên Internet phải tuân thủ các quy định của pháp luật về bảo đảm an toàn thông tin và các quy định của cơ quan, tổ chức.

b) Khi cài đặt, kết nối máy tính/thiết bị đầu cuối phải thực hiện theo hướng dẫn/quy trình dưới sự giám sát của bộ phận chuyên trách về an toàn thông tin.

c) Máy tính/thiết bị đầu cuối phải được xử lý điểm yếu an toàn thông tin, cấu hình cứng hóa bảo mật trước khi kết nối vào hệ thống.

2. Trong quá trình sử dụng

a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao.

b) Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng.

c) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách công nghệ thông tin của nhà trường để kịp thời ngăn chặn và xử lý.

d) Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng được cấp trên hoặc đơn vị chuyên môn tổ chức.

Scanned with OKEN Scanner

Điều 18. Các hành vi nghiêm cấm khi sử dụng mạng nội bộ, Thư công vụ:

1. Nghiêm cấm cắm các thiết bị lạ, truyền mạng wifi cá nhân.

2. Ngăn chặn việc truyền tải thông tin trên mạng, can thiệp, truy nhập, gây nguy hại, xóa, thay đổi, sao chép và làm sai lệch thông tin trên mạng trái pháp luật.

3. Gây ảnh hưởng, cản trở trái pháp luật tới hoạt động bình thường của hệ thống thông tin hoặc tới khả năng truy nhập hệ thống thông tin của người sử dụng.

4. Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của biện pháp bảo vệ an toàn thông tin mạng của hệ thống thông tin; tấn công, chiếm quyền điều khiển, phá hoại hệ thống thông tin.

5. Không sử dụng thư công vụ vào việc riêng

Điều 19. Kiểm tra, đánh giá và quản lý rủi ro an toàn thông tin

1. Nội dung kiểm tra, đánh giá và quản lý rủi ro an toàn thông tin

a) Kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ.

b) Đánh giá hiệu quả của biện pháp bảo đảm an toàn hệ thống thông tin.

c) Đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống.

d) Kiểm tra, đánh giá khác do chủ quản hệ thống thông tin quy định.

2. Hình thức kiểm tra, đánh giá và quản lý rủi ro an toàn thông tin

a) Định kỳ theo quy định của pháp luật và kế hoạch của chủ quản hệ thống thông tin.

b) Kiểm tra, đánh giá đột xuất theo yêu cầu của cấp có thẩm quyền.

Điều 20. Phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin

1. Thiết bị CNTT có chứa dữ liệu (máy tính, thiết bị lưu trữ, ...) khi bị hỏng phải được cán bộ vận hành 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.

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

3. Các phương tiện và thiết bị CNTT: Máy tính cá nhân (PC), máy tính xách tay, máy chủ, các thiết bị mạng, phương tiện lưu trữ như CD/DVD, thẻ nhớ, ổ cứng phải xóa sạch dữ liệu khi chuyển giao hoặc thay đổi mục đích sử dụng

CHƯƠNG IV

Scanned with OKEN Scanner

TỔ CHỨC THỰC HIỆN

Điều 21. Trách nhiệm của các thành viên trong nhà trường

1. Trách nhiệm chung của các thành viên tham gia sử dụng hệ thống công nghệ thông tin

Tất cả các thành viên tham gia sử dụng hệ thống công nghệ thông tin trong nhà trường phải bảo mật tài khoản sử dụng, không nhờ người khác làm thay công việc của mình, thường xuyên thay đổi mật khẩu đăng nhập. Ngoài ra phải thực hiện một số nhiệm vụ khác do hiệu trưởng yêu cầu.

2. Trách nhiệm của hiệu trưởng

- Tiến hành việc thiết lập phân quyền hệ thống người dùng, phù hợp với quyền hạn nhiệm vụ công tác cho từng thành viên, cán bộ, giáo viên, nhân viên trong nhà trường đảm bảo nhiệm vụ phân công theo điều lệ trường học.

- Ban hành quyết định thành lập Ban CNTT tại nhà trường

- Thành lập ban biên tập website của nhà trường trong đó hiệu trưởng là trưởng ban, thành viên là lãnh đạo các tổ chức đoàn thể chính quyền trong nhà trường chỉ đạo các tổ bộ phận trong nhà trường viết bài, đưa tin của nhà trường đảm bảo sự sinh động website từng ngày, tháng đồng thời sử dụng hiệu quả các tính năng của website.

- Chỉ đạo việc cung cấp thông tin định kỳ và thông báo đột xuất cho phụ huynh học sinh về kết quả giáo dục và tình trạng sức khỏe của mỗi học sinh.

- Xây dựng quy chế sử dụng phần mềm trong đó quy định rõ về thời điểm khóa, mở và quy định các thủ tục, thời gian cập nhật điểm số, nhận xét đánh giá sau khi khóa sổ.

- Xét duyệt học sinh được lên lớp, không được lên lớp, danh hiệu thi đua, phải kiểm tra lại các môn học trong kỳ nghỉ hè, kết quả đánh giá học sinh trên phần mềm Quản lý nhà trường SMAS khi tất cả giáo viên bộ môn và giáo viên chủ nhiệm lớp đã cập nhật đầy đủ nội dung thông tin.

- Chỉ đạo công tác lưu trữ và bảo quản sổ theo dõi và đánh giá học sinh (theo lớp); các hồ sơ đề nghị sửa chữa thông tin, điểm số của từng năm học; quản lý học bạ học sinh trong thời gian học sinh học tập tại nhà trường.

- Việc lưu trữ, bảo quản tài liệu chuyên môn nghiệp vụ, hồ sơ sổ sách, giáo án, học bạ điện tử… được thực hiện theo quy định tại Thông tư số 27/2016/TT-BGDĐT ngày 30/12/2016 của Bộ Giáo dục và Đào tạo.

- Quyết định xử lý theo thẩm quyền đề nghị các cấp có thẩm quyền quyết định xử lý đối với tổ chức cá nhân vi phạm, quyết định khen thưởng theo thẩm quyền đề nghị cấp có thẩm quyền khen thưởng đối với tổ chức cá nhân có thành tích trong việc thực hiện quy định này.

3. Trách nhiệm của quản trị hệ thống (đ/c Phạm Thị Thu Thường)

Scanned with OKEN Scanner

- Xây dựng kế hoạch kiểm tra, tổ chức kiểm tra, đánh giá việc cập nhật hồ sơ, sổ sách của giáo viên trên phần mềm Quản lý nhà trường SMAS và các phần mềm tương tự như: Kế hoạch giáo dục của tổ chuyên môn, kế hoạch giáo dục của cá nhân, kế hoạch bài dạy của giáo viên, sổ chủ nhiệm…

- Giám sát việc vào điểm kiểm tra định kỳ và kiểm tra thường xuyên của giáo viên và các bộ môn trong toàn trường theo kế hoạch dựa vào phổ điểm qua các bài kiểm tra để chỉ đạo công tác dạy và học ở mỗi bộ một phù hợp.

- Hàng tháng kiểm tra đánh giá học sinh trên hệ thống của các Gv.

- Báo cáo với hiệu trưởng các trường hợp bất thường về điểm số và phối hợp với các tổ nhóm chuyên môn để xử lý.

- Đôn đốc các tổ chuyên môn và giúp hiệu trưởng phê duyệt nội dung các bài viết về chuyên môn được đăng tải trên website của nhà trường.

- Phê duyệt việc sửa thông tin, điểm số của giáo viên và Ban quản trị phần mềm Quản lý nhà trường SMAS (theo mẫu *Giấy đề nghị thay đổi thông tin*).

- Quản lý, chỉ đạo công tác in sổ điểm, học bạ, thống kê chất lượng và lưu trữ theo quy định.

- Khởi tạo và quản lý tất cả các tài khoản sử dụng phần mềm Quản lý nhà trường SMAS, website tại đơn vị; kiểm tra việc thực hiện các quy định về phân quyền, bảo mật tài khoản.

- Quản lý và chịu trách nhiệm về việc điều chỉnh các sai sót trong quá trình nhập thông tin, điểm số trên phần mềm Quản lý nhà trường SMAS, CSDL ngành sau khi khóa dữ liệu.

- Phân quyền cho các cá nhân, tổ, nhóm, bộ phận sử dụng phần mềm.

- Quản lý và bảo mật dữ liệu, thực hiện khóa/mở sổ theo yêu cầu của hiệu trưởng nhà trường.

- Cập nhật dữ liệu ban đầu vào đầu mỗi năm học hoặc khi có thay đổi theo sự phân công của hiệu trưởng trên phần mềm Quản lý nhà trường SMAS, CSDL ngành, website.

- Tập huấn, hướng dẫn, hỗ trợ giáo viên, nhân viên trong việc sử dụng phần mềm.

- Thực hiện thao tác chuyển trường, tiếp nhận, chuyển cấp học đối với học sinh trên hệ thống SMAS, CSDL ngành.

- Trích xuất thông tin, dữ liệu gửi về Sở/ để tổng hợp, phục vụ báo cáo quản lý chuyên ngành.

- Quản lý hệ thống mạng, đường truyền internet, hệ thống máy tính và các thiết bị phục vụ công tác ứng dụng CNTT nhà trường.

Scanned with OKEN Scanner

- Lập kế hoạch chuẩn bị CSVC đáp ứng Hội nghị, hội thảo trực tuyến; sinh hoạt chuyên môn và thao giảng trực tuyến trong cụm, trường và các ứng dụng CNTT trong dạy và học.

4. Trách nhiệm của tổ trưởng chuyên môn

- Kiểm tra đôn đốc việc thực hiện các quy định về hồ sơ sổ sách điện tử cập nhật điểm và các thông tin khác của các tổ viên trên hệ thống của nhà trường.

- Phân công người viết bài đưa tin và chịu trách nhiệm về tính chính xác của nội dung các hoạt động chuyên môn của tổ nhóm chuyên môn mà mình phụ trách theo kế hoạch trên website của nhà trường.

- Xây dựng kế hoạch và tổ chức thực hiện những việc sinh hoạt chuyên môn thao giảng trực tuyến trong trường và các ứng dụng công nghệ thông tin vào dạy học thẩm định các sản phẩm sinh hoạt theo chuyên đề chủ đề do giáo viên tổ nhóm biên soạn trước khi đăng tải trên website của nhà trường.

- Đề nghị với hiệu trưởng và cấp có thẩm quyền xử phạt và đề nghị khen thưởng cá nhân có thành tích tốt thực hiện quy định này.

5. Trách nhiệm của giáo viên chủ nhiệm

a) Chịu trách nhiệm trước hiệu trưởng về việc bảo mật thông tin tài khoản của mình trong quá trình sử dụng.

b) Cập nhật vào hệ thống phần mềm Quản lý nhà trường các thông tin:

- Danh sách và sơ yếu lý lịch học sinh đầu năm học.

- Kiểm diện học sinh định kỳ hàng tuần, hàng tháng.

- Đánh giá học học sinh thường xuyên, định kì.

- Các thông tin liên quan khác trên phần mềm.

c) Thực hiện chức năng: Kiểm tra lại các kết quả đánh giá, xếp loại định kì học sinh trên phần mềm.

d) Kiểm tra và ký xác nhận các nội dung sau dây:

- Kết quả kiểm diện học sinh trong năm học.

- Kết quả đánh giá, xếp loại năng lực và phẩm chất của học sinh.

- Kết quả được lên lớp hoặc ở lại lớp, công nhận học sinh khen thưởng trong năm học, được lên lớp sau khi kiểm tra lại hoặc rèn luyện trong hè; xét đề xuất các hình thức khen thưởng của học sinh.

- Cập nhật thành tích và khen thưởng, nhận xét vào HBĐT.

- Sổ theo dõi và đánh giá học sinh, học bạ học sinh.

- Hướng dẫn học sinh ứng dụng công nghệ thông tin vào học tập khuyến khích học sinh tham gia viết bài và đưa tin trên website của nhà trường động viên học sinh tham gia các cuộc thi trực tuyến do Bộ, Sở giáo dục đào tạo phát động. Hướng dẫn học sinh tham gia học tập trên OLM.

Scanned with OKEN Scanner

- Báo tin nhắn kịp thời cho cha mẹ học sinh (CMHS) tình hình học tập và rèn luyện mỗi tuần, tháng và những thông báo đột xuất khác thông qua ứng dụng liên lạc điện tử giữa Nhà trường và CMHS.

6. Trách nhiệm của giáo viên bộ môn

- Chịu trách nhiệm trước hiệu trưởng về việc bảo mật thông tin tài khoản của mình trong quá trình sử dụng.

- Trực tiếp nhập kết quả đánh giá, xếp loại học sinh của các lớp được phân công giảng dạy vào phần mềm, đảm bảo chính xác với Sổ theo dõi và đánh giá học sinh (theo lớp và theo giáo viên).

- Báo cáo với TTCM về các vấn đề sự cố liên quan đến hệ thống phần mềm hoặc các vấn đề khó khăn khác khi tiến hành cập nhập thông tin, điểm số, nhận xét, đánh giá.

- Thực hiện thao giảng trực tuyến soạn giảng Elearning, thiết kế học liệu số và các ứng dụng công nghệ thông tin vào dạy học. Biên soạn các sản phẩm sinh hoạt theo chuyên đề chủ đề nhóm phân công.

- Tham gia viết bài và đưa tin trên website của nhà trường theo sự phân công của tổ nhóm chuyên môn và các tổ chức đoàn thể trong nhà trường.

7. Trách nhiệm của nhân viên kế toán

- Chịu trách nhiệm trước hiệu trưởng về việc bảo mật thông tin tài khoản của mình, các phần mềm được giao quản lý trong quá trình sử dụng.

- Tiến hành cài đặt phần mềm quản lý kế toán triển khai nhập thông tin hồ sơ chứng từ hằng năm theo quy định.

- Cập nhật đầy đủ tài sản và hệ thống quản lý tài sản theo quy định.

- Cập nhật đầy đủ thông tin hồ sơ viên chức, người lao động đào tạo bồi dưỡng quá trình công tác nâng lương khen thưởng kỉ luật và phần mềm của hệ thống phần mềm tương ứng.

- Đăng tải các nội dung công khai của nhà trường theo quy định.

8. Trách nhiệm giáo viên kiêm thư viện, văn thư, thiết bị

- Chịu trách nhiệm trước hiệu trưởng về việc bảo mật thông tin tài khoản, phần mềm giao quản lý trong quá trình sử dụng.

- Cập nhật hệ thống quản lý văn bản điều hành trên hộp thư điện tử để báo cáo lãnh đạo nhà trường xử lý đúng thời hạn, Sắp xếp lưu trữ văn bản hồ sơ theo quy định khoa học.

- Thực hiện việc chỉnh sửa văn bằng, chứng chỉ, chuyển đến, chuyển đi trên hệ thống dịch vụ công trực tuyến.

- Cập nhật thư mục sách, tài liệu trên phần mềm quản lý thư viện trường học. Hàng năm tăng cường, bổ sung nguồn học liệu lưu hành nội bộ cho thư viện (đề kiểm tra định kỳ, sáng kiến kinh nghiệm, tài liệu tập huấn các cấp . . .)

Scanned with OKEN Scanner

9. Trách nhiệm phụ trách Y tế trường học

- Chịu trách nhiệm trước hiệu trưởng về việc bảo mật thông tin tài khoản, phần mềm giao quản lý trong quá trình sử dụng.

- Cập nhật theo dõi sức khỏe định kỳ cho học sinh trên hệ thống phần mềm Quản lý nhà trường.

- Tư vấn cho phụ huynh học sinh trong việc chăm sóc sức khỏe học sinh tại nhà và sổ liên lạc điện tử, thông báo cho phụ huynh những thông tin về bệnh lý học sinh thường gặp như các tật khúc xạ về mắt suy dinh dưỡng còi xương…

- Cập nhật đầy đủ các thông tin về thiết bị y tế danh mục và số lượng các loại thuốc được trang bị hằng năm.

Điều 22. Rà soát, cập nhật, bổ sung quy chế

1. Quy chế này thay thế cho quy chế quản lý, sử dụng hệ thống công nghệ thông tin trong nhà trường ban hành kèm theo Quyết định số 57/QĐ-THMT ngày 24/02/2025.

2. Định kỳ hàng năm hoặc khi có thay đổi chính sách an toàn thông Ban CNTT nhà trường kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung Quy chế bảo đảm an toàn thông tin.

3. Có hồ sơ lưu lại thông tin phản hồi của viên chức, người lao động trong quá trình triển khai, áp dụng chính sách an toàn thông tin./.

Scanned with OKEN Scanner