UBND HUYỆN MƯỜNG CHÀ
TRƯỜNG PTDTBT TH MƯỜNG ANH

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

Số: 06a/QĐ-PTDTBT-THMA

Pa Ham, ngày 20 tháng 02 năm 2025

QUYẾT ĐỊNH
Ban hành Quy chế đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin

HIỆU TRƯỞNG TRƯỜNG PTDTBT TIỂU HỌC MƯỜNG ANH

Căn cứ Luật An toàn thông tin mạng ngày 19/11/2015; Căn cứ Luật An ninh mạng ngày 12/6/2018;

Căn cứ Luật Bảo vệ bí mật nhà nước ngày 15/11/2018;

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

Thực hiện Kế hoạch số 01a/KH-PTDTBT-THMA ngày 24/01/2025 của trường PTDTBT TH Mường Anh về việc thực hiện nhiệm vụ ứng dụng công nghệ thông tin và chuyển đổi số

Theo đề nghị của tổ ứng dụng CNTT và chuyển đổi số.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế Bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của trường PTDTBT tiểu học Mường Anh.

Điều 2. Tổ chức thực hiện

Tổ trưởng các tổ chuyên môn, văn phòng, cá nhân có tham gia vào nền tảng chung của trường, ngành có trách nhiệm triển khai thực hiện nghiêm túc Quy chế này.

Điều 3. Quyết định này có hiệu lực từ ngày ký.

Các tổ Chuyên môn, tổ văn phòng, cá nhân trong nhà trường chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Phòng GD&ĐT (b/c);
- Lưu: VT, CM.

P. HIỆU TRƯỞNG

Nguyễn Thị Nga

QUY CHẾ
Đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin
(Ban hành kèm theo QĐ số 50/QĐ-PTDTBT-THMA ngày 20/2 /2025 của trường PTDTBT TH Mường Anh)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi và đối tượng áp dụng

1. Quy chế này quy định về đảm bảo An toàn thông tin mạng trong các hoạt động ứng dụng công nghệ thông tin của Trường PTDTBT tiểu học Mường Anh.

2. Quy chế này áp dụng đối với:

a. Cán bộ giáo viên, nhân viên, người lao động trường PTDTBT TH Mường Anh

b. Các tổ chuyên môn, tổ văn phòng, cá nhân có sử dụng hoặc kết nối truy cập vào hệ thống mạng của đơn vị, các hệ thống thông tin thuộc trường PTDTBT tiểu học Mường Anh.

c. Cơ quan, tổ chức, cá nhân cung cấp dịch vụ quản lý, vận hành, bảo trì, phát triển và đảm bảo an toàn thông tin mạng cho đơn vị.

Điều 2. Mục đích, nguyên tắc bảo đảm an toàn thông tin mạng

Việc áp dụng Quy chế này nhằm phòng ngừa, ngăn chặn, xử lý và giảm các nguy cơ gây mất an toàn thông tin mạng và bảo đảm an ninh thông tin trong quá trình ứng dụng công nghệ thông tin, chuyển đổi số trong hoạt động của đơn vị.

Hoạt động ứng dụng công nghệ thông tin, chuyển đổi số của cơ quan, đơn vị phải tuân thủ theo nguyên tắc bảo đảm an toàn thông tin mạng được quy định tại Điều 4, Luật An toàn thông tin mạng ngày 19/11/2015 và Điều 41 Nghị định 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.

Điều 3. Giải thích từ ngữ

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

Hệ thống mạng: bao gồm dịch vụ kết nối Internet; mạng nội bộ.

Mạng nội bộ (LAN): là tập hợp các trang thiết bị công nghệ thông tin được kết nối với nhau thông qua các bộ chuyển mạch, bộ định tuyến, bộ điểm truy cập và các máy chủ, thiết bị quản lý mạng, phần mềm quản lý mạng, thiết bị an toàn hệ thống mạng trong phạm vi quản lý của trường. Mạng nội bộ bao gồm mạng nội bộ có dây và mạng nội bộ không dây (Wifi).

Hệ thống thông tin được quy định tại Khoản 3, Điều 3, Luật An toàn thông tin mạng. Cụ thể: Hệ thống thông tin 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.

An toàn thông tin mạng: là sự bảo vệ thông tin số và các 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.

Phần mềm độc hại được quy định tại Khoản 11, Điều 3, Luật An toàn thông tin mạng. Cụ thể: Phần mềm độc hại là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay 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.

Trang thiết bị công nghệ thông tin cá nhân: bao gồm máy tính để bàn, máy tính

xách tay, thiết bị số (máy tính bảng, điện thoại thông minh) của cá nhân.

Điều 4. Phạm vi đảm bảo an toàn thông tin

Hệ thống mạng.

Hệ thống thông tin quản lý, gồm: các phần mềm nghiệp vụ và cơ sở dữ liệu phục vụ công tác quản lý, điều hành hoạt động của trường.

Trang thiết bị công nghệ thông tin cá nhân.

Điều 5. Nguyên tắc đảm bảo an toàn thông tin mạng

Đảm bảo an toàn thông tin mạng là yêu cầu bắt buộc, thường xuyên, liên tục, có tính xuyên suốt quá trình, đồng bộ từ khi thiết kế, xây dựng, vận hành, nâng cấp và hủy bỏ hệ thống thông tin. Đảm bảo an toàn thông tin mạng phải tuân thủ các nguyên tắc chung, được quy định tại Điều 4 Luật An toàn thông tin mạng và Điều 4 Nghị định số 85/2016/NĐ-CP ngày 01/07/ 2016 của Chính phủ.

Việc vận hành hệ thống thông tin đảm bảo các yêu cầu về an toàn thông tin mạng và sẵn sàng xử lý sự cố an toàn thông tin mạng đối với các hệ thống thông tin; bố trí nhân sự chuyên trách chịu trách nhiệm bảo đảm an toàn, an ninh thông tin mạng.

Xác định rõ quyền hạn, trách nhiệm của Lãnh đạo cơ quan, từng bộ phận, cá nhân trong đơn vị có liên quan đối với công tác bảo đảm an toàn thông tin mạng trong phạm vi xử lý công việc của mình theo quy định của Nhà nước và của trường PTDTBT tiểu học Mường Anh.

Thông tin mật, thông tin thuộc Danh mục bí mật Nhà nước phải được bảo vệ theo quy định của Nhà nước và các quy định khác về công tác bảo vệ bí mật Nhà nước và các nội dung tương ứng trong Quy chế này.

Xử lý sự cố an toàn thông tin mạng phải phù hợp với trách nhiệm, quyền hạn và đảm bảo lợi ích hợp pháp của đơn vị, cá nhân liên quan và theo quy định của pháp luật.

Điều 6. Các hành vi bị nghiêm cấm

Các hành vi nghiêm cấm quy định tại Điều 7 Luật An toàn thông tin mạng, Điều 8 Luật An ninh mạng, Điều 5 Luật Bảo vệ bí mật nhà nước.

Tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập mạng không dây của cá nhân vào mạng nội bộ; trên cùng một thiết bị thực hiện đồng thời truy cập vào mạng nội bộ và truy cập Internet bằng thiết bị kết nối Internet của cá nhân (3G/4G, điện thoại di động, máy tính bảng, máy tính xách tay).

Tự ý thay đổi, gỡ bỏ biện pháp an toàn thông tin cài đặt trên thiết bị công nghệ thông tin phục vụ công việc; tự ý thay thế, lắp mới, tráo đổi thành phần của máy tính phục vụ công việc.

Tạo ra, cài đặt, phát tán phần mềm độc hại.

Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của. Các hành vi khác có tính chất cố tình làm mất an toàn, bí mật thông tin của đơn vị, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

Chương II
QUY ĐỊNH ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 7. Bảo vệ bí mật Nhà nước trong hoạt động ứng dụng công nghệ thông tin

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

Không được sử dụng máy tính hoặc các thiết bị khác đã kết nối hoặc đang kết

nối với mạng Internet, mạng máy tính, mạng viễn thông, trừ trường hợp lưu trữ bí mật Nhà nước theo quy định của pháp luật về cơ yếu để soạn thảo, chuyển giao, lưu trữ tài liệu có nội dung bí mật Nhà nước; cung cấp tin, tài liệu có nội dung bí mật Nhà nước trên mạng xã hội (Zalo; Telegram; Facebook; ...) và đưa thông tin có nội dung bí mật Nhà nước trên Cổng/Trang thông tin điện tử.

Không được in, sao chụp tài liệu có nội dung bí mật Nhà nước trên các thiết bị có kết nối mạng internet, mạng máy tính, mạng viễn thông, trừ trường hợp theo quy định của pháp luật về cơ yếu.

Phải bố trí ít nhất 01 máy tính riêng và phải được kiểm tra an ninh, an toàn thông tin, không kết nối mạng Internet, mạng máy tính, mạng viễn thông, trừ trường hợp theo quy định của pháp luật về cơ yếu dùng để quản lý, lưu trữ, soạn thảo các tài liệu có nội dung bí mật Nhà nước.

Khi sửa chữa, khắc phục các sự cố của máy tính dùng soạn thảo, lưu trữ tài liệu có nội dung bí mật Nhà nước, cá nhân phụ trách phải báo cáo cho người có thẩm quyền cho ý kiến. Không được thuê, hợp đồng, cho phép các tổ chức, cá nhân không có trách nhiệm trực tiếp sửa chữa, xử lý, khắc phục sự cố.

Trước khi thanh lý các máy tính tại nhà trường giáo viên, nhân viên phụ trách công nghệ thông tin phải tháo ổ cứng (thanh lý không kèm ổ cứng hoặc các thiết bị lưu trữ khác gắn kèm) và dùng các biện pháp kỹ thuật chuyên biệt để xoá bỏ vĩnh viễn dữ liệu lưu trữ trong ổ cứng, các thiết bị lưu trữ khác gắn kèm hoặc phá hủy về mặt vật lý ổ cứng, các thiết bị lưu trữ khác nếu chứa các tài liệu có nội dung bí mật Nhà nước.

Điều 8. Quy định về cấp phát, thu hồi, cập nhật và quản lý các tài khoản truy cập vào hệ thống thông tin dùng chung của trường

Mỗi cá nhân, tổ chuyên môn được cấp các tài khoản truy cập các ứng dụng dùng chung của đơn vị, gắn với cá nhân đó, đơn vị đó và chỉ truy cập vào các Trang/Cổng thông tin điện tử, ứng dụng trực tuyến phù hợp với chức năng, trách nhiệm, quyền hạn của mình. Trường hợp sử dụng tài khoản dùng chung cho một nhóm người hay một đơn vị, phải có cơ chế xác định các cá nhân, đơn vị có trách nhiệm quản lý tài khoản. Người dùng chỉ được truy cập các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình và có trách nhiệm bảo mật tài khoản truy cập được cấp.

Tài khoản quản trị hệ thống (mạng máy tính, hệ điều hành, thiết bị kết nối mạng, phần mềm ứng dụng, cơ sở dữ liệu, hệ thống thông tin) phải tách biệt với tài khoản truy cập của người sử dụng thông thường. Tài khoản hệ thống phải được giao đích danh cá nhân làm công tác quản trị.

Bộ phận, viên chức, người lao động được giao quản trị các hệ thống thông tin cấp, khóa quyền truy cập của tài khoản các hệ thống thông tin trong trường hợp tài khoản đó thực hiện các hành vi tấn công hoặc để xảy ra vấn đề mất an toàn thông tin, an ninh mạng.

Trường hợp viên chức, người lao động thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ hưu, trong vòng không quá 05 ngày làm việc sau khi có quyết định của cấp có thẩm quyền thì đơn vị quản lý cá nhân đó phải thông báo cơ quan, đơn vị, người có thẩm quyền để điều chỉnh, thu hồi, hủy bỏ các quyền sử dụng đối với hệ thống thông tin.

Mật mã đăng nhập, truy cập hệ thống thông tin có độ dài tối thiểu 08 ký tự, bao gồm ký tự in hoa, ký tự in thường, ký tự chữ số và ký tự đặc biệt (!, @, #, %, $, *, &)

được quy định tại Điều 7 của Quyết định số 1305/QĐ-UBND ngày 14/7/2022 của Ủy ban nhân dân huyện.

Các tổ chuyên môn, cá nhân rà soát tối thiểu 03 tháng/lần các tài khoản đăng nhập, bảo đảm các tài khoản và quyền truy cập hệ thống được cấp phát đúng, đủ.

Điều 9. Bảo đảm nguồn nhân lực

Giáo viên, nhân viên chuyên trách về công nghệ thông tin được bảo đảm các điều kiện học tập, tiếp cận công nghệ, kiến thức an toàn bảo mật thông tin trước khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ.

Giáo viên, nhân viên được giao nhiệm vụ quản lý, vận hành truy cập, khai thác đối với các hệ thống thông tin thực hiện 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; 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.

Thường xuyên tổ chức, phổ biến các quy định về bảo đảm an toàn thông tin nhằm nâng cao nhận thức về trách nhiệm bảo đảm an toàn thông tin cho cán bộ giáo viên, nhân viên sử dụng hệ thống thông tin do đơn vị quản lý.

Điều 10. Bảo đảm an toàn hạ tầng mạng

Quản lý hạ tầng mạng nội bộ:

Tuân thủ các quy định kiến trúc hệ thống, tiêu chuẩn, quy chuẩn kỹ thuật; cài đặt, cấu hình, tổ chức hệ thống mạng phù hợp với các tiêu chuẩn ứng dụng công nghệ thông tin của các cơ quan Nhà nước, bảo đảm an toàn thông tin; hạn chế sử dụng mô hình mạng có nguy cơ mất an toàn thông tin cao.

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. Trang bị thiết bị tường lửa hoặc phần mềm tường lửa để ngăn chặn và phát hiện xâm nhập trái phép vào mạng nội bộ của đơn vị khi kết nối với hệ thống bên ngoài; ưu tiên sử dụng các sản phẩm, giải pháp, dịch vụ an toàn thông tin mạng do doanh nghiệp Việt Nam sản xuất hoặc làm chủ công nghệ.

Đối với các đơn vị không nằm cùng một khu vực thì cần thiết lập mạng riêng ảo (VPN) để tăng cường an ninh cho hạ tầng mạng nội bộ. 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/mở cổng giao tiếp mạng, giao thức và các dịch vụ không cần thiết.

Khi thực hiện truy cập từ xa vào mạng nội bộ để thực hiện chức năng quản trị, phải sử dụng giao thức mạng có mã hóa thông tin (như: SSL/TLS, VPN...) và thiết lập mật khẩu có độ phức tạp cao.

Xây dựng quy trình kết nối thiết bị đầu cuối của người sử dụng vào hệ thống mạng; truy cập và quản lý cấu hình hệ thống; cấu hình tối ưu, tăng cường bảo mật cho thiết bị mạng, bảo mật trong hệ thống và thực hiện quy trình trước khi đưa hệ thống vào vận hành khai thác.

Cá nhân, tổ chuyên môn, tổ văn phòng phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng.

Quản lý hệ thống mạng không dây:

Khi thiết lập mạng không dây để kết nối với mạng cục bộ thông qua các điểm

truy nhập (Access Point - AP), cơ quan, đơn vị vận hành phải thiết lập các tham số: Tên, nhận dạng dịch vụ (Service Set Identifier - SSID), mật khẩu phải đặt theo quy định tại Điều 7 của Quyết định số 1305/QĐ-UBND ngày 14/7/2022 của UBND huyện, cấp phép truy nhập đối với địa chỉ vật lý (MAC Address), mã hóa dữ liệu theo cơ chế bảo mật WPA2 hoặc WPA3.

Mật khẩu đăng nhập phải được thiết lập có độ phức tạp cao, định kỳ 6 tháng thay đổi mật khẩu nhằm tăng cường công tác bảo mật.

Khi cung cấp truy cập Internet qua mạng không dây cho Camera hoặc người ngoài, cơ quan, đơn vị sử dụng phải phân VLAN riêng với một SSID riêng và giới hạn băng thông truy cập phù hợp đối với đối tượng.

Điều 11. Bảo đảm an toàn dữ liệu

Quản lý tài khoản: Khi cấp tài khoản lần đầu cho người dùng truy nhập, người dùng phải thay đổi mật khẩu sau khi đăng nhập thành công lần đầu.

Các hệ thống thông tin khi phân quyền phải thiết lập chế độ giới hạn số lần đăng nhập không hợp lệ vào hệ thống tối đa không quá 05 lần, khi người dùng đăng nhập sai vượt quá số lần quy định, tài khoản chuyển sang chế độ khóa quyền truy cập; các hệ thống thông tin xác lập chế độ thoát ra khỏi hệ thống nếu người sử dụng không tương tác trên hệ thống của phiên làm việc quá 15 phút.

Chủ tài khoản không chia sẻ, giao quyền tài khoản và mật khẩu truy nhập cho người khác. Không sử dụng tài khoản của người khác để đăng nhập vào hệ thống thông tin, cơ sở dữ liệu.

Tài khoản thư điện tử cá nhân, nhà trường theo tên miền dienbien.edu.vn để phục vụ cho các hoạt động mang tính nghiệp vụ, không sử dụng để giao dịch, đăng ký trên mạng xã hội, các trang thông tin điện tử công cộng khác.

Tài khoản quản trị hệ thống được giao cho giáo viêc, nhân viên chuyên trách về công nghệ thông tin phục vụ cho công tác quản trị, phân quyền, cấu hình hệ thống đó. Phụ trách quản trị hệ thống không sử dụng cùng một mật khẩu cho nhiều tài khoản khác nhau.

Khi cá nhân thay đổi vị trí công tác, chuyển công tác, thôi việc, nghỉ hưu thì báo cho cơ quan, đơn vị vận hành thực hiện khoản 4 Điều 7 Quy chế này về điều chỉnh, thu hồi, hủy bỏ tài khoản.

Cơ chế mã hóa và sao lưu dữ liệu phải bảo đảm tính toàn vẹn của dữ liệu.

Các đơn vị khi triển khai dịch vụ sao lưu dự phòng ở mức vật lý cần thiết lập chức năng RAID (Redundant Arrays of Inexpensive Disks hoặc Redundant rrays of Independent Disks) để tăng tốc độ đọc/ghi hoặc bảo đảm khả năng lưu trữ dự phòng.

Đối với công tác 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):

Lập danh sách các dữ liệu, phần mềm cần 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.

Xây dựng tài liệu, quy trình hướng dẫn sao lưu/phục hồi dữ liệu của hệ thống: Đơn vị quản trị hệ thống thực hiện xây dựng Tài liệu hướng dẫn sao lưu cụ thể đối với từng hệ thống cung cấp dịch vụ, hệ thống điều hành mà đơn vị quản lý.

Giáo viên, nhân viên chuyên trách về công nghệ thông tin phối hợp với các cơ

quan, 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), phần mềm ứng dụng, cơ sở dữ liệu, tệp tin ghi nhật ký 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.

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 bảo đảm sẵn sàng cho việc sử dụng khi cần; việc kiểm tra, phục hồi hệ thống từ dữ liệu sao lưu tối thiểu 3 tháng một lần (hoặc khi có yêu cầu đột xuất).

Khi thực hiện chia sẻ tài nguyên trên máy trạm đơn vị vận hành phải sử dụng mật khẩu để bảo vệ thông tin, dữ liệu; không thực hiện chia sẻ toàn bộ ổ cứng; theo dõi, giám sát để kết thúc chia sẻ tài nguyên ngay khi hoàn thành. Các thông tin, tài liệu, dữ liệu nhạy cảm phải được mã hóa trước khi trao đổi, truyền nhận qua mạng máy tính.

Thông tin, dữ liệu thuộc phạm vi bí mật Nhà nước phải được quản lý theo Điều 7 của Quy chế này.

Điều 12. Bảo đảm an toàn thiết bị đầu cuối

Trên máy tính cá nhân phải thiết lập chế độ tự động cập nhật hệ điều hành trên máy tính, phải thiết lập mật khẩu truy cập chế độ tự động bảo vệ màn hình khi không sử dụng; sử dụng những trình duyệt an toàn, đáng tin cậy, cài đặt phần mềm phòng, chống mã độc; thiết lập chế độ tự động cập nhật phần mềm phòng, chống mã độc, chế độ tự động rà quét mã độc khi sao chép, mở các tập tin, chế độ rà quét máy tính định kỳ hằng tuần.

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

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 đơn vị.

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 của đơn vị. Các máy tính truy cập mạng Internet phải cài đặt phần mềm giám sát mã độc.

Trong quá trình sử dụng thiết bị đầu cuối: 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.

Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà cá nhân được giao sử dụng.

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 đơn vị để kịp thời ngăn chặn và xử lý.

Điều 13. Quản lý giám sát an toàn hệ thống thông tin

Chủ quản hệ thống thông tin phải triển khai hệ thống giám sát an toàn thông tin đáp ứng các yêu cầu tại Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin.

Đối với các hệ thống thông tin, phần mềm, ứng dụng, cơ sở dữ liệu không được đặt tại Trung tâm tích hợp dữ liệu tỉnh, huyện thì chủ quản hệ thống thông tin có trách nhiệm tự thực hiện hoặc yêu cầu doanh nghiệp cung cấp dịch vụ bảo đảm các yêu cầu giám sát an toàn hệ thống thông tin theo quy định của pháp luật.

Thông tin giám sát mã độc phải được chia sẻ với Trung tâm Giám sát an toàn không gian mạng quốc gia do Bộ Thông tin và Truyền thông quản lý theo quy định của pháp luật và hướng dẫn của Sở, Bộ Thông tin và Truyền thông.

Định kỳ hàng năm tổ chức đánh giá, kiểm tra đối với hệ thống thông tin nội bộ tại đơn vị. Thực hiện các biện pháp bảo trì cần thiết để bảo đảm khả năng xử lý và tính sẵn sàng của hệ thống thông tin.

Điều 14. Ứng cứu sự cố an toàn thông tin

Nguyên tắc ứng cứu xử lý sự cố: Chủ động, kịp thời, nhanh chóng, chính xác, đồng bộ và hiệu quả.

Phối hợp chặt chẽ, tuân thủ quy định của pháp luật về điều phối ứng cứu sự cố an toàn thông tin.

Ứng cứu xử lý sự cố trước hết phải được thực hiện, xử lý bằng lực lượng tại chỗ và trách nhiệm chính của chủ quản hệ thống thông tin.

Việc xử lý sự cố an toàn thông tin phải bảo đảm quyền và lợi ích hợp pháp của đơn vị, cá nhân, bảo mật thông tin cá nhân, thông tin riêng của đơn vị khi tham gia các hoạt động ứng cứu xử lý sự cố.

Phân nhóm sự cố an toàn thông tin:

Sự cố do bị tấn công mạng: Tấn công từ chối dịch vụ; tấn công giả mạo; tấn công sử dụng mã độc; truy cập trái phép, chiếm quyền điều khiển; tấn công thay đổi giao diện; tấn công mã hóa phần mềm, dữ liệu, thiết bị; phá hoại thông tin, dữ liệu, phần mềm; nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu; các hình thức tấn công mạng khác.

Sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật.

Sự cố do lỗi của người quản trị, vận hành hệ thống.

Sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn.

Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin: hoạt động ứng cứu sự cố an toàn thông tin mạng huy động các nguồn lực nằm ngoài phạm vi của đơn vị vận hành hệ thống thông tin để đối phó với các sự cố quy định tại khoản 1 Điều này.

Phân loại mức độ sự cố:

Thấp: sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của đơn vị.

Trung bình: sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hay đình trệ hoạt động chính của đơn vị.

Cao: sự cố tác động đến khả năng vận hành của hệ thống thông tin, ảnh hưởng đến dữ liệu, thiết bị, gây ảnh hưởng đến hoạt động chung của đơn vị và hoạt động cung cấp dịch vụ công cho HS, GV, người lao động, phụ huynh học sinh.

Nghiêm trọng: sự cố gây gián đoạn hoặc đình trệ hệ thống trong một khoảng thời gian ngắn, ảnh hưởng nghiêm trọng đến dữ liệu, thiết bị của hệ thống, gây thiệt hại nghiêm trọng cho đơn vị.

Đặc biệt nghiêm trọng: sự cố làm tê liệt toàn bộ hoạt động của hệ thống, gây

thiệt hại đặc biệt nghiêm trọng cho đơn vị, HS, phụ huynh, GV, NV, người lao động, đe dọa trật tự an toàn xã hội.

Quy trình phối hợp ứng cứu xử lý sự cố:

Bước 1: Nếu hệ thống có nguy cơ mất an toàn thông tin mạng thuộc thẩm quyền đơn vị trực tiếp quản lý thì thực hiện tiếp.

Bước 2. Nếu hệ thống có nguy cơ mất an toàn thông tin mạng thuộc Trung tâm Công nghệ thông tin và Truyền thông trực thuộc Sở Thông tin và Truyền thông quản lý (các hệ thống được triển khai tập trung tại Trung tâm tích hợp Dữ liệu tỉnh) thì thực hiện tiếp Bước 3.

Bước 3: Tiến hành xử lý sự cố theo quy chế nội bộ của cơ quan, đơn vị. Nếu sự cố được khắc phục thì lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố. Khi sự cố vượt quá khả năng xử lý của cơ quan, đơn vị, lập biên bản ghi nhận và thực hiện tiếp Bước 4.

Bước 4: Báo sự cố đến bộ phận vận hành hệ thống thông tin cơ quan, Phòng GD&ĐT, UBND huyện để phối hợp Sở Thông tin và Truyền thông xử lý.

Trường hợp có sự cố nghiêm trọng ở mức độ cao, khẩn cấp hoặc vượt quá khả năng khắc phục của đơn vị: lãnh đạo đơn vị phải báo cáo ngay cho cơ quan cấp trên quản lý trực tiếp để được hướng dẫn, hỗ trợ.

Giáo viên, nhân viên chuyên trách về an toàn thông tin có trách nhiệm:

Xây dựng phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng, ứng phó sự cố an toàn thông tin mạng.

Xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định.

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;

Tổ chức tập huấn, diễn tập phương án xử lý sự cố an toàn thông tin theo chỉ đạo của Lãnh đạo.

Chương III
TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG VÀ TỔ CHỨC THỰC HIỆN

Điều 15. Trách nhiệm của Trường PTDTBT tiểu học Mường Anh.

Ban chỉ đạo về ứng dụng CNTT-Chuyển đổi số Trường PTDTBT TH Mường Anh.

(thành lập theo QĐ số 11/QĐ-PTDTBT-THMA ngày 11/9/2024 của trường PTDTBT tiểu học Mường Anh) đảm nhiệm chức năng Ban chỉ đạo ứng cứu khẩn cấp sự cố an toàn thông tin mạng trong nhà trường và có trách nhiệm, quyền hạn thực hiện theo quy định tại Điều 5 Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ về ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia.

Hàng năm, cử viên chức tham gia các lớp đào tạo, tập huấn về công tác bảo đảm an toàn thông tin mạng cho cán bộ phụ trách an toàn thông tin mạng. Tổ chức tuyên truyền về an toàn thông tin mạng trong công tác quản lý Nhà nước trong nhà trường.

Điều 16. Trách nhiệm của đơn vị vận hành hệ thống thông tin

Thực hiện trách nhiệm của đơn vị vận hành hệ thống thông tin theo quy định tại Quy chế này và các nhiệm vụ do chủ quản hệ thống thông tin phân công.

Chỉ đạo, phân công giáo viên, nhân viên thuộc đơn vị (quản lý ứng dụng; quản lý dữ liệu; vận hành hệ thống thông tin; triển khai và hỗ trợ kỹ thuật) triển khai công tác bảo đảm an toàn thông tin trong tất cả các công đoạn liên quan đến hệ thống thông tin.

Điều 17. Trách nhiệm của viên chức, người lao động trong nhà trường

Trách nhiệm của giáo viên, nhân viên phụ trách về an toàn thông tin/công nghệ thông tin tại đơn vị:

Chịu trách nhiệm bảo đảm an toàn thông tin mạng của đơn vị.

Tham mưu lãnh đạo đơn vị ban hành các quy chế, quy trình nội bộ, triển khai các giải pháp kỹ thuật bảo đảm an toàn thông tin mạng.

Thực hiện việc giám sát, đánh giá, báo cáo Lãnh đạo đơn vị các rủi ro mất an toàn thông tin mạng và mức độ nghiêm trọng của các rủi ro đó.

Phối hợp với các cá nhân, đơn vị có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn thông tin mạng.

Thường xuyên cập nhật nâng cao kiến thức, trình độ chuyên môn đáp ứng yêu cầu bảo đảm an toàn thông tin mạng của đơn vị.

Trách nhiệm của người sử dụng:

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.

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

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 đơn vị để kịp thời ngăn chặn và xử lý.

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

Điều 18. Tổ chức thực hiện

Căn cứ Quy chế này, Tổ trưởng chuyên môn, văn phòng các tổ có trách nhiệm tổ chức tuyên truyền, phổ biến cho toàn thể giáo viên, nhân viên, người lao động triển khai thực hiện trong phạm vi quản lý.

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

Trong quá trình thực hiện Quy chế, nếu có vấn đề vướng mắc, phát sinh, các đơn vị phản ánh kịp thời về Tổ CNTT để được hướng dẫn thực hiện./.

PHỤ LỤC

Danh mục mẫu biểu quy định ứng cứu sự cố an toàn thông tin mạng

(Ban hành kèm theo QĐ số /QĐ-PTDTBT-THMA, ngày 20/2/2025 của Trường PTDTBT tiểu học Mường Anh)

STT	Mẫu số	Tên mẫu biểu
1	Mẫu số 01	Báo cáo ban đầu sự cố an toàn thông tin mạng
2	Mẫu số 02	Báo cáo kết thúc ứng phó sự cố

MẪU SỐ 01
BÁO CÁO BAN ĐẦU SỰ CỐ MẠNG

THÔNG TIN VỀ TỔ CHỨC/CÁ NHÂN BÁO CÁO SỰ CỐ
Tên tổ chuyên môn/cá nhân báo cáo sự cố (*):.....
Địa chỉ: (*) .....
Điện thoại (*) .....Email (*).....
NGƯỜI LIÊN HỆ
Họ và tên (*).....Chức vụ: .....
Điện thoại (*) .....Email (*) .....
THÔNG TIN CHI TIẾT VỀ HỆ THỐNG BỊ SỰ CỐ

Tên đơn vị vận hành hệ thống thông tin (*):	Điền tên đơn vị vận hành hoặc được thuê vận hành hệ thống thông tin
Tổ chuyên môn:	Điền tên tổ chuyên môn
Tên hệ thống bị sự cố	Điền tên hệ thống bị sự cố và tên miền, địa chỉ ip liên quan
Phân loại cấp độ của hệ thống thông tin, (nếu có)	Cấp độ 1□ Cấp độ 2 □ Cấp độ 3 □ Cấp độ 4 □ Cấp độ 5□
Tổ chức cung cấp dịch vụ an toàn thông tin (nếu có):	Điền tên nhà cung cấp ở đây
Tên nhà cung cấp dịch vụ kết nối bên ngoài (nếu có)	Điền tên nhà cung cấp ở đây
Dải địa chỉ Public IP kết nối với hệ thống bên ngoài:	Điền thông tin ở đây
Mô tả sơ bộ về sự cố (*)	
Đề nghị cung cấp một bản tóm tắt ngắn gọn về sự cố, bao gồm đánh giá sơ bộ cuộc tấn công đã xảy ra chưa và bất kỳ các nguy cơ dẫn đến khả năng phá hoại hoặc gián đoạn dịch vụ. Cũng vui lòng xác định mức độ nhạy cảm của thông tin liên quan hoặc những đối tượng bị ảnh hưởng bởi sự cố:	

Ngày phát hiện sự cố (*): / / (dd/mm/yyyy)	Thời gian phát hiện (*):	……giờ.....phút

HIỆN TRẠNG SỰ CỐ (*)
□ Đã được xử lý □ Chưa được xử lý
CÁCH THỨC PHÁT HIỆN * (Đánh dấu những cách thức được sử dụng để phát hiện sự cố)
□ Qua hệ thống phát hiện xâm nhập □ Kiểm tra dữ liệu lưu lại (Log File)
Nhận được thông báo từ .....
Khác, đó là .....
ĐÃ GỬI THÔNG BÁO SỰ CỐ CHO *
Thành viên mạng lưới chịu trách nhiệm ứng cứu sự cố cho tổ chức, cá nhân ISP đang trực

tiếp cung cấp dịch vụ □
Cơ quan điều phối □

THÔNG TIN BỔ SUNG VỀ HỆ THỐNG XẢY RA SỰ CỐ

Hệ điều hành..... Version.....
Các dịch vụ có trên hệ thống *(Đánh dấu những dịch vụ được sử dụng trên hệ thống)*
Web server □ Mail server □ Database server
Dịch vụ khác, đó là .....
Các biện pháp an toàn thông tin đã triển khai *(Đánh dấu những biện pháp đã triển khai)*
Antivirus □ Firewall □ Hệ thống phát hiện xâm nhập
Khác: .....
Các địa chỉ IP của hệ thống
(Liệt kê địa chỉ IP sử dụng trên Internet, không liệt kê địa chỉ IP nội bộ)
Các tên miền của hệ thống .....
Mục đích chính sử dụng hệ thống .....
Thông tin gửi kèm
Nhật ký hệ thống □ Mẫu virus /mã độc
Khác: .....
Các thông tin cung cấp trong thông báo sự cố này đều phải được giữ bí mật:
Có □ Không □

KIẾN NGHỊ, ĐỀ XUẤT HỖ TRỢ

Mô tả về đề xuất, kiến nghị
Đề nghị cung cấp tóm lược về các kiến nghị và đề xuất hô trợ ứng cứu (nếu có) ……..……..……..… ……..……..……..…… ……..……..……..…… ……..…….. ……

THỜI GIAN THỰC HIỆN BÁO CÁO SỰ CỐ (ngày/tháng/năm/giờ/phút):

CÁ NHÂN/NGƯỜI ĐẠI DIỆN THEO PHÁP LUẬT
(Ký, ghi rõ họ tên)

MẪU SỐ 02
BÁO CÁO KẾT THÚC ỨNG PHÓ SỰ CỐ

THÔNG TIN VỀ TỔ CHỨC/CÁ NHÂN BÁO CÁO
Tên tổ chuyên môn/cá nhân báo cáo sự cố (*).....
Địa chỉ: (*) .....
Điện thoại (*) ..... Email (*) .....
KÝ HIỆU BÁO CÁO BAN ĐẦU SỰ CỐ:
Số ký hiệu..... Ngày báo cáo: / / 20...
THÔNG TIN CHI TIẾT VỀ HỆ THỐNG BỊ SỰ CỐ

Tên đơn vị vận hành hệ thống thông tin (*):	*Điền tên đơn vị vận hành hoặc được thuê vận hành hệ thống thông tin*				
Tổ chuyên môn:	*Điền tên tổ chuyên môn*				
Tên hệ thống bị sự cố	*Điền tên hệ thống bị sự cố*				
Phân loại cấp độ của hệ thống thông tin, (nếu có)	□ Cấp độ 1	□ Cấp độ 2	□ Cấp độ 3	□ Cấp độ 4	□ Cấp độ 5
Tên/Mô tả về sự cố					
Ngày phát hiện sự cố / / (dd/mm/yy)		Thời gian phát hiện (*):		..... giờ phút	
Kết quả xử lý sự cố					
Cung cấp, tóm tắt tổng quát về những gì đã xảy ra và cách thức giải quyết, đề xuất giải pháp ứng cứu ứng sự cố nhằm xử lý nhanh sự cố, giảm nhẹ rủi ro và thiệt hại đối với sự cố tương tự trong tương lai...					
Các tài liệu đính kèm					
Liệt kê các tài liệu liên quan (báo cáo diễn biến sự cố; phương án xử lý, log file...)					

CÁ NHÂN/NGƯỜI ĐẠI DIỆN THEO PHÁP LUẬT
(Ký, ghi họ tên)