UBND XÃ YÊN MÔ **TRƯỜNG MN YÊN HƯNG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT N** **Độc lập - Tự do - Hạnh phúc**
Số: 76/QĐ-TrMN	*Yên Mô, ngày 03 tháng 4 năm 2026*

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an ninh mạng, an toàn thông tin đối với hệ thống thông tin thuộc phạm vi quản lý của Trường Mầm non Yên Hưng Năm học 2025-2026

HIỆU TRƯỞNG TRƯỜNG MẦM NON YÊN HƯNG

Căn cứ Luật Công nghệ thông tin số 67/2006/QH11;

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

Căn cứ Luật An ninh mạng số 24/2018/QH14;

Căn cứ Luật Bảo vệ bí mật nhà nước số 29/2018/QH14;

Căn cứ Quyết định số 14/2026/QĐ-UBND ngày 30/01/2026 của Uỷ ban nhân dân tỉnh Ninh Bình về việc ban hành quy chế bảo đảm an ninh mạng, an toàn thông tin đối với hệ thống thông tin trên địa bàn tỉnh Ninh Bình;

Căn cứ Quyết định số 1122/QĐ-UBND ngày 22/10/2025 của Uỷ ban nhân dân tỉnh Ninh Bình ban hành Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Giáo dục và Đào tạo tỉnh Ninh Bình;

Căn cứ Quyết định số 363/QĐ-SGDĐT ngày 04/03/2026 của SGD&ĐT tỉnh Ninh Bình ban hành Quy chế bảo đảm an ninh mạng, an toàn thông tin đối với hệ thống thông tin thuộc phạm vi quản lý của Sở Giáo dục và Đào tạo;

Xét đề nghị của bộ phận chuyên môn Trường Mầm non Yên Hưng.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an ninh mạng, an toàn thông tin đối với hệ thống thông tin thuộc phạm vi quản lý của Trường Mầm non Yên Hưng.

Điều 2. Quy chế này áp dụng đối với toàn thể cán bộ quản lý, giáo viên, nhân viên và các cá nhân sử dụng hệ thống thông tin của nhà trường.

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

Điều 4. Các tổ chức đoàn thể, các tổ chuyên môn và cán bộ, giáo viên, nhân viên của nhà trường chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Cấp ủy Cb (để b/c);
- Như điều 4;
- Lưu VT.

HIỆU TRƯỞNG

TRƯỜNG MẦM NON YÊN HƯNG

Phan Thị Lâm Hà

QUY CHẾ

Bảo đảm an ninh mạng, an toàn thông tin đối với hệ thống thông tin thuộc phạm vi quản lý của Trường Mầm non Yên Hưng

(Ban hành kèm theo Quyết định số 76. /QĐ-Tr.MN ngày 13./03/2026 của Hiệu trưởng Trường Mầm non Yên Hưng)

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 về việc bảo đảm an ninh mạng và an toàn thông tin đối với các hệ thống thông tin, mạng máy tính, cơ sở dữ liệu và thiết bị công nghệ thông tin thuộc phạm vi quản lý của Trường Mầm non Yên Hưng.

2. Đối tượng áp dụng

Áp dụng đối với tất cả cán bộ, giáo viên, nhân viên và các tổ chức, cá nhân tham gia khai thác, sử dụng hệ thống thông tin của nhà trường.

Điều 2. Giải thích từ ngữ

1. An ninh mạng là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân theo quy định của Luật An ninh mạng.

2. An toàn thông tin là sự 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.

3. Hệ thống thông tin của nhà trường: Bao gồm máy tính, mạng nội bộ, internet, phần mềm quản lý, cơ sở dữ liệu và các thiết bị công nghệ thông tin khác, 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. Sự cố an toàn thông tin là sự việc xảy ra gây mất an toàn thông tin hoặc có nguy cơ gây mất an toàn thông tin đối với hệ thống thông tin, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.

5. Người sử dụng hệ thống thông tin là cán bộ quản lý, giáo viên, nhân viên của nhà trường được cấp quyền truy cập và sử dụng các thiết bị, phần mềm hoặc hệ thống thông tin của đơn vị.

6. 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.

7. Ứng cứu sự cố an toàn thông tin mạng là hoạt động nhằm xử lý, khắc phục sự cố gây mất an toàn thông tin mạng gồm: Theo dõi, thu thập, phân tích, phát hiện, cảnh

báo, điều tra, xác minh sự cố, ngăn chặn sự cố, khôi phục dữ liệu và khôi phục hoạt động bình thường của hệ thống thông tin.

Điều 3. Nguyên tắc bảo đảm an ninh mạng, an toàn thông tin

Việc bảo đảm an ninh mạng, an toàn thông tin phải tuân thủ các quy định của pháp luật, đặc biệt là Luật An ninh mạng và Luật An toàn thông tin mạng.

Bảo đảm an ninh mạng, an toàn thông tin phải được thực hiện thường xuyên, liên tục trong quá trình quản lý, vận hành và khai thác hệ thống thông tin của nhà trường.

Thông tin, dữ liệu của nhà trường, đặc biệt là thông tin liên quan đến trẻ em, cán bộ, giáo viên, nhân viên phải được bảo vệ, không để lộ, mất hoặc bị truy cập trái phép.

Việc sử dụng hệ thống thông tin phải đúng mục đích phục vụ công tác quản lý, giảng dạy và các hoạt động giáo dục của nhà trường.

Mỗi cán bộ quản lý, giáo viên và nhân viên có trách nhiệm thực hiện các quy định về bảo đảm an ninh mạng, an toàn thông tin và kịp thời báo cáo khi phát hiện nguy cơ mất an toàn thông tin.

Điều 4. Các hành vi bị nghiêm cấm

1. Lợi dụng không gian mạng, hệ thống thông tin của nhà trường để thực hiện các hành vi vi phạm pháp luật, xâm phạm lợi ích của Nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân theo quy định của Luật An ninh mạng.

2. Truy cập trái phép, chiếm quyền điều khiển, phá hoại hoặc làm gián đoạn hoạt động của hệ thống thông tin, mạng máy tính của nhà trường.

3. Phát tán virus máy tính, phần mềm độc hại hoặc các chương trình có khả năng gây mất an toàn thông tin đối với hệ thống thông tin.

4. Tự ý cài đặt phần mềm không rõ nguồn gốc, phần mềm không phục vụ công việc trên máy tính của nhà trường.

5. Tiết lộ, cung cấp, đăng tải thông tin nội bộ, thông tin cá nhân của trẻ em, cán bộ, giáo viên, nhân viên khi chưa được phép của người có thẩm quyền theo quy định của Luật Bảo vệ bí mật nhà nước.

6. Sử dụng mạng Internet, mạng xã hội để đăng tải, chia sẻ thông tin sai sự thật, thông tin chưa được kiểm chứng gây ảnh hưởng đến uy tín của nhà trường hoặc ngành giáo dục.

7. Sử dụng hệ thống thông tin của nhà trường vào mục đích cá nhân không phù hợp với môi trường giáo dục.

8. Hành vi khác bị nghiêm cấm theo quy định của pháp luật.

Chương II
QUY ĐỊNH BẢO ĐẢM AN NINH MẠNG, AN TOÀN THÔNG TIN

Điều 5. Bảo đảm an ninh mạng, an toàn thông tin khi sử dụng máy tính và thiết bị ngoại vi

1. Máy tính và thiết bị ngoại vi phải được cài đặt hệ điều hành, phần mềm văn phòng, phần mềm chuyên dụng phục vụ công việc và tuân thủ các quy định của pháp luật về công nghệ thông tin, an toàn thông tin mạng theo Luật Công nghệ thông tin và Luật An toàn thông tin mạng.

a) Chỉ cài đặt phần mềm hợp lệ, có nguồn gốc rõ ràng, được phép sử dụng theo quy định của pháp luật; không cài đặt các phần mềm không rõ nguồn gốc, phần mềm vi phạm bản quyền hoặc không phục vụ cho công việc của nhà trường theo quy định của Luật Công nghệ thông tin và Luật An toàn thông tin mạng.

b) Cài đặt phần mềm phòng, chống và xử lý phần mềm độc hại trên máy tính của nhà trường; thiết lập chế độ tự động cập nhật cơ sở dữ liệu nhận diện mã độc nhằm kịp thời phát hiện, ngăn chặn và xử lý các nguy cơ gây mất an toàn thông tin theo quy định của Luật An toàn thông tin mạng.

c) Khi phát hiện bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy tính (máy chạy chậm bất thường, cảnh báo từ phần mềm phòng, chống phần mềm độc hại, mất dữ liệu,...), phải cô lập máy tính (ngắt kết nối mạng vật lý, tắt máy) và báo trực tiếp cho Tổ trưởng tổ văn phòng được nhà trường giao phụ trách an ninh mạng, an toàn thông tin của nhà trường để được xử lý kịp thời.

d) Chỉ truy nhập vào các trang thông tin điện tử, cổng thông tin điện tử, hệ thống thông tin và các ứng dụng trực tuyến tin cậy; bảo đảm việc truy cập, khai thác thông tin phù hợp với chức năng, nhiệm vụ, quyền hạn được giao và phục vụ hoạt động quản lý, giảng dạy của nhà trường theo quy định của Luật An toàn thông tin mạng; không truy nhập, mở các trang tin, thư điện tử không rõ nguồn gốc; không sử dụng tính năng lưu mật khẩu tự động hoặc đăng nhập tự động trên các máy tính dùng chung.

đ) Có trách nhiệm bảo mật tài khoản truy nhập hệ thống thông tin; không chia sẻ tài khoản, mật khẩu hoặc thông tin cá nhân liên quan đến việc đăng nhập cho người khác. Mật khẩu phải được thiết lập bảo đảm độ an toàn cao, tối thiểu 08 ký tự bao gồm chữ thường, chữ in hoa, chữ số và ký tự đặc biệt (ví dụ: @, #, !,…); thực hiện thay đổi mật khẩu định kỳ tối thiểu 06 tháng một lần. Các tài khoản truy cập hệ thống phải được đăng xuất khi không sử dụng; đồng thời thường xuyên xóa bộ nhớ tạm (cache) và cookie của trình duyệt trên máy tính nhằm hạn chế nguy cơ mất an toàn thông tin theo quy định của Luật An toàn thông tin mạng.

e) Thực hiện thao tác khóa máy tính bằng các chức năng bảo mật có sẵn trên hệ điều hành khi tạm thời rời khỏi vị trí làm việc; tắt máy tính và các thiết bị liên quan khi

kết thúc thời gian làm việc hoặc khi rời khỏi cơ quan nhằm bảo đảm an toàn thông tin và tránh truy cập trái phép vào hệ thống thông tin của nhà trường.

2. Trước khi mang máy tính, thiết bị công nghệ thông tin cá nhân có kết nối mạng đến nơi làm việc và kết nối với mạng nội bộ của nhà trường để phục vụ xử lý công việc, cá nhân phải báo cáo và được sự đồng ý của Hiệu trưởng hoặc người được Hiệu trưởng phân công phụ trách. Trong trường hợp này, cá nhân phải tuân thủ đầy đủ các quy định và chịu sự kiểm tra, giám sát của Tổ trưởng tổ văn phòng được nhà trường giao phụ trách công nghệ thông tin, an ninh mạng, an toàn thông tin của đơn vị.

3. Đối với thiết bị soạn thảo, lưu trữ bí mật nhà nước

a) Việc soạn thảo, in ấn, lưu trữ tài liệu có nội dung thuộc danh mục bí mật nhà nước phải được thực hiện trên máy tính độc lập và sử dụng máy in, máy photocopy không kết nối và không có lịch sử kết nối với mạng Internet, mạng máy tính hoặc mạng viễn thông, trừ trường hợp lưu giữ bí mật nhà nước theo quy định của pháp luật về cơ yếu để soạn thảo, lưu trữ các văn bản có nội dung bí mật nhà nước.

b) Cá nhân được giao nhiệm vụ trong quá trình xử lý công việc, soạn thảo văn bản có nội dung bí mật nhà nước chỉ được sử dụng máy tính và các thiết bị theo quy định tại điểm a khoản này. Việc lưu trữ tài liệu có nội dung bí mật nhà nước phải được thực hiện trên các thiết bị lưu trữ riêng biệt, bảo đảm các yêu cầu về bảo vệ bí mật nhà nước và cơ yếu theo quy định của Luật Bảo vệ bí mật nhà nước.

Điều 6. Quản lý trang thiết bị công nghệ thông tin, an toàn, an ninh thông tin đối với cá nhân

1. Quản lý trang thiết bị công nghệ thông tin đối với cá nhân

a) Các cá nhân có trách nhiệm quản lý trang thiết bị công nghệ thông tin trong phạm vi được giao phụ trách.

b) Trang thiết bị công nghệ thông tin có lưu trữ dữ liệu nhạy cảm khi thay đổi mục đích sử dụng hoặc thanh lý phải được kiểm tra và thực hiện các biện pháp xóa, tiêu hủy dữ liệu bảo đảm không có khả năng khôi phục lại. Việc thực hiện do Tổ trưởng tổ văn phòng được nhà trường giao phụ trách công nghệ thông tin. Trường hợp không thể xóa hoặc tiêu hủy hoàn toàn dữ liệu, nhà trường phải thực hiện tiêu hủy bộ phận lưu trữ dữ liệu của thiết bị để bảo đảm an toàn thông tin theo quy định của Luật An toàn thông tin mạng.

c) Thiết bị tính toán có bộ phận lưu trữ hoặc các thiết bị lưu trữ dữ liệu khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài hoặc khi ngừng sử dụng phải tháo bộ phận lưu trữ ra khỏi thiết bị hoặc thực hiện xóa toàn bộ thông tin, dữ liệu lưu trữ trên thiết bị, bảo đảm không làm lộ lọt thông tin. Trường hợp cần thiết phải giữ lại dữ liệu để phục vụ việc khôi phục hoặc xử lý kỹ thuật thì phải thực hiện các biện pháp bảo đảm an toàn thông tin theo quy định của Luật An toàn thông tin mạng.

d) Tổ trưởng tổ văn phòng được nhà trường giao phụ trách công nghệ thông tin có trách nhiệm định kỳ kiểm tra, sửa chữa, bảo trì các trang thiết bị công nghệ thông tin của nhà trường; đồng thời hướng dẫn cán bộ quản lý, giáo viên và nhân viên sử dụng, quản lý và vận hành các thiết bị, hệ thống công nghệ thông tin đúng quy định, bảo đảm an toàn, an ninh thông tin theo quy định của Luật An toàn thông tin mạng.

2. Quản lý an ninh mạng, an toàn thông tin đối với cá nhân

a) Nhà trường có trách nhiệm xác định các yêu cầu và trách nhiệm bảo đảm an ninh mạng, an toàn thông tin đối với từng vị trí công việc của cán bộ quản lý, giáo viên và nhân viên. Khi tuyển dụng hoặc tiếp nhận nhân sự mới, nhà trường phải phổ biến, hướng dẫn các quy định về bảo đảm an ninh mạng, an toàn thông tin của đơn vị. Đối với các vị trí có liên quan đến việc quản lý, khai thác dữ liệu quan trọng hoặc quản trị hệ thống thông tin của nhà trường, cá nhân được giao nhiệm vụ phải thực hiện cam kết bảo mật thông tin bằng văn bản hoặc thực hiện theo các quy trình làm việc có các biện pháp bảo mật nhằm bảo đảm an toàn thông tin theo quy định của Luật An toàn thông tin mạng.

b) Nhà trường có trách nhiệm thường xuyên phổ biến, quán triệt các quy định về an ninh mạng, an toàn thông tin cho cán bộ quản lý, giáo viên và nhân viên nhằm nâng cao nhận thức, trách nhiệm của từng cá nhân trong việc bảo đảm an ninh mạng, an toàn thông tin trong quá trình sử dụng và khai thác hệ thống thông tin của đơn vị theo quy định của Luật An toàn thông tin mạng.

c) Khi có nhu cầu cấp mới, thay đổi, quản lý hoặc thu hồi tài khoản truy cập các hệ thống thông tin, các bộ phận chuyên môn hoặc cá nhân có liên quan phải báo cáo Ban giám hiệu hoặc Tổ trưởng tổ văn phòng được nhà trường giao phụ trách công nghệ thông tin để thực hiện việc cấp, quản lý, phân quyền truy cập và thu hồi tài khoản cũng như các tài sản liên quan đến hệ thống thông tin của nhà trường theo quy định của Luật An toàn thông tin mạng.

d) Khi cán bộ quản lý, giáo viên hoặc nhân viên của nhà trường chấm dứt công tác, chuyển công tác hoặc thay đổi vị trí công việc, phải thực hiện lập biên bản bàn giao các trang thiết bị công nghệ thông tin, tài khoản và các tài sản liên quan đến hệ thống thông tin. Nhà trường có trách nhiệm thông báo cho Tổ trưởng tổ văn phòng được giao phụ trách công nghệ thông tin để thực hiện việc thay đổi, điều chỉnh hoặc thu hồi quyền truy cập các hệ thống thông tin của đơn vị, bảo đảm an toàn thông tin theo quy định của Luật An toàn thông tin mạng.

Điều 7. An toàn thông tin mạng đối với thuê dịch vụ công nghệ thông tin

1. Khi tham mưu ký kết hợp đồng thuê dịch vụ công nghệ thông tin, Tổ trưởng tổ văn phòng phụ trách công nghệ thông tin của nhà trường phải phối hợp với các bộ phận liên quan tham mưu Ban Giám hiệu thực hiện ký kết hợp đồng với đơn vị cung cấp dịch vụ. Nội dung hợp đồng phải quy định rõ phạm vi dịch vụ, trách nhiệm, quyền hạn và nghĩa vụ của các bên trong việc bảo đảm an toàn thông tin mạng; đồng thời có điều

khoản về xử lý vi phạm và trách nhiệm bồi thường thiệt hại do vi phạm của bên cung cấp dịch vụ gây ra.

2. Trách nhiệm của Tổ trưởng tổ văn phòng phụ trách công nghệ thông tin của nhà trường trong quá trình sử dụng dịch vụ công nghệ thông tin

a) Yêu cầu bên cung cấp dịch vụ thực hiện bảo mật thông tin, dữ liệu, mã nguồn và tài liệu thiết kế của hệ thống; triển khai các biện pháp bảo đảm an toàn thông tin theo quy định của Quy chế này, Luật An toàn thông tin mạng, Luật An ninh mạng và các quy định pháp luật có liên quan.

b) Thực hiện giám sát việc cung cấp dịch vụ; quản lý và giới hạn quyền truy cập của bên cung cấp dịch vụ khi được phép truy cập vào hệ thống thông tin của nhà trường.

c) Khi phát hiện bên cung cấp dịch vụ có dấu hiệu vi phạm quy định về bảo đảm an toàn thông tin:

- Báo cáo Ban Giám hiệu nhà trường và xem xét tạm dừng hoặc đình chỉ hoạt động của bên cung cấp dịch vụ theo mức độ vi phạm.
- Thu hồi ngay quyền truy cập hệ thống thông tin đã cấp cho bên cung cấp dịch vụ.
- Kiểm tra, xác định mức độ vi phạm và thiệt hại (nếu có), lập báo cáo và tham mưu Ban Giám hiệu xử lý vi phạm, yêu cầu bồi thường thiệt hại theo quy định của hợp đồng và pháp luật.

3. Trách nhiệm của các bộ phận trong nhà trường khi kết thúc sử dụng dịch vụ công nghệ thông tin

a) Thông báo cho Tổ trưởng tổ văn phòng phụ trách công nghệ thông tin của nhà trường thực hiện thu hồi quyền truy cập hệ thống thông tin và các tài sản liên quan đã cấp cho bên cung cấp dịch vụ; đồng thời thay đổi các khóa, tài khoản và mật khẩu truy cập hệ thống thông tin.

b) Phối hợp với Tổ trưởng tổ văn phòng phụ trách công nghệ thông tin yêu cầu bên cung cấp dịch vụ chuyển giao đầy đủ các thông tin, dữ liệu, mã nguồn, tài liệu thiết kế và các công cụ cần thiết nhằm bảo đảm nhà trường có thể tiếp tục khai thác, sử dụng hệ thống thông tin liên tục, kể cả trong trường hợp thay đổi đơn vị cung cấp dịch vụ.

Điều 8. Xác định cấp độ và phương án bảo đảm an ninh mạng, an toàn thông tin hệ thống thông tin

Tổ trưởng tổ văn phòng phụ trách công nghệ thông tin của nhà trường có trách nhiệm tham mưu Ban Giám hiệu tổ chức thực hiện việc xác định cấp độ và triển khai các phương án bảo đảm an ninh mạng, an toàn thông tin đối với các hệ thống thông tin của nhà trường theo quy định của Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ; Nghị định 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ và Thông tư 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông.

Điều 9. Ứng cứu sự cố an toàn hệ thống thông tin

1. Nguyên tắc ứng cứu xử lý sự cố

a) Chủ động, kịp thời, nhanh chóng, chính xác, đồng bộ và hiệu quả.

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

c) Ưu tiên ứng cứu, xử lý sự cố bằng lực lượng tại chỗ và trách nhiệm chính của chủ quản hệ thống thông tin, đơn vị vận hành 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 tập thể, cá nhân; bảo mật thông tin cá nhân, thông tin riêng của cơ quan khi tham gia các hoạt động ứng cứu xử lý sự cố.

2. Phân loại sự cố an toàn thông tin mạng

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

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

c) Sự cố do lỗi của cán bộ quản trị, vận hành hệ thống.

d) Sự cố do các thảm họa tự nhiên.

3. Phân loại mức độ sự cố

a) Thấp: sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của cơ quan.

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

c) 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 cơ quan.

d) 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 cơ quan.

đ) Đặc biệt nghiêm trọng: sự cố làm tê liệt toàn bộ hoạt động của hệ thống, gây thiệt hại đặc biệt nghiêm trọng cho cơ quan và đe dọa trật tự an toàn xã hội.

4. Quy trình ứng cứu sự cố thực hiện theo Điều 11 Thông tư số 20/2017/TT-BTTTT.

5. Quá trình xử lý sự cố phải được ghi chép và lưu trữ tại đơn vị; bảo toàn bằng chứng, chứng cứ phục vụ cho việc kiểm tra, xử lý, khắc phục và phòng ngừa sự cố. Trong trường hợp sự cố có liên quan đến các vi phạm pháp luật, đơn vị có trách nhiệm thu thập và cung cấp chứng cứ cho cơ quan có thẩm quyền theo quy định của pháp luật.

Điều 10. Quản lý rủi ro, lỗ hổng, điểm yếu an ninh mạng, an toàn thông tin

1. Tổ trưởng tổ văn phòng được Hiệu trưởng phân công công nghệ thông tin làm đầu mối chủ trì, phối hợp với các bộ phận, cá nhân có liên quan trong nhà trường để tổ

chức quản lý lỗ hổng, điểm yếu an ninh mạng, an toàn thông tin, bao gồm các nội dung sau:

a) Lập danh sách toàn bộ thiết bị và phần mềm công nghệ thông tin đang sử dụng trong phạm vi quản lý của Trường Mầm non, bao gồm: Nhãn hiệu phần cứng (máy tính, máy chủ, thiết bị mạng, thiết bị lưu trữ) tên phần mềm và phiên bản đang sử dụng (hệ điều hành, phần mềm quản lý, cơ sở dữ liệu, phần mềm ứng dụng và các tiện ích khác).

b) Tiếp nhận thông tin về lỗ hổng, điểm yếu an toàn an ninh mạng từ các cơ quan, tổ chức có chức năng cảnh báo về an toàn an ninh mạng như: Bộ Thông tin và Truyền thông, Sở Thông tin và Truyền thông, Sở Giáo dục và Đào tạo, cơ quan công an và các đơn vị có thẩm quyền.

c) Quản lý, giám sát việc cài đặt bản vá lỗ hổng, điểm yếu an toàn an ninh mạng. Triển khai cài đặt bản vá lỗ hổng, điểm yếu an toàn an ninh mạng sau khi bản vá được phát hành; Áp dụng các biện pháp bảo vệ tạm thời trong trường hợp bản vá bảo mật chưa được phát hành hoặc chưa đủ điều kiện để triển khai.

2. Các tổ chuyên môn, bộ phận hành chính và cá nhân sử dụng hệ thống thông tin của nhà trường có trách nhiệm phối hợp với Tổ trưởng tổ văn phòng phụ trách công nghệ thông tin trong việc quản lý rủi ro an toàn thông tin, thực hiện các biện pháp phòng ngừa, phát hiện và khắc phục lỗ hổng, điểm yếu an ninh mạng theo quy định và hướng dẫn của cơ quan có thẩm quyền.

3. Trên cơ sở kết quả kiểm tra, đánh giá an toàn thông tin mạng hoặc cảnh báo nguy cơ mất an toàn thông tin từ cơ quan có thẩm quyền như Công an, Sở Thông tin và Truyền thông, Sở Giáo dục và Đào tạo hoặc các cơ quan liên quan, Tổ trưởng tổ văn phòng phụ trách công nghệ thông tin của nhà trường có trách nhiệm: Tham mưu Hiệu trưởng tổ chức khắc phục các tồn tại, nguy cơ mất an toàn thông tin, Trường hợp cần thiết, đề xuất lựa chọn đơn vị có đủ năng lực chuyên môn để triển khai các phương án khắc phục, Sau khi hoàn thành việc xử lý, báo cáo kết quả thực hiện với Hiệu trưởng và cơ quan quản lý cấp trên theo quy định để theo dõi, tổng hợp.

Điều 11. Đào tạo, bồi dưỡng nghiệp vụ, tuyên truyền, phổ biến nâng cao nhận thức về an ninh mạng, an toàn thông tin.

1. Tổ trưởng tổ văn phòng phụ trách công nghệ thông tin của nhà trường được Hiệu trưởng phân công chủ trì, tham mưu Hiệu trưởng tổ chức hoặc phối hợp tổ chức đào tạo, bồi dưỡng nghiệp vụ về an ninh mạng, an toàn thông tin cho cán bộ, giáo viên, nhân viên trong nhà trường, bao gồm: Bồi dưỡng kiến thức, kỹ năng cơ bản về an toàn thông tin mạng cho cán bộ quản lý, giáo viên, nhân viên sử dụng máy tính và các hệ thống thông tin của nhà trường; Tập huấn, hướng dẫn cho cán bộ phụ trách công nghệ thông tin hoặc cán bộ phụ trách chuyển đổi số trong nhà trường về các biện pháp bảo đảm an ninh mạng, an toàn thông tin trong quá trình quản lý, vận hành hệ thống thông tin.

2. Các tổ chuyên môn, bộ phận và cá nhân trong nhà trường có trách nhiệm phối hợp với Tổ trưởng tổ văn phòng phụ trách công nghệ thông tin trong việc tuyên truyền,

phổ biến và nâng cao nhận thức về an ninh mạng, an toàn thông tin, cụ thể: Thường xuyên tuyên truyền, phổ biến các quy định của pháp luật và quy chế của nhà trường về bảo đảm an ninh mạng, an toàn thông tin; nâng cao ý thức trách nhiệm của cán bộ, giáo viên, nhân viên trong việc sử dụng thiết bị công nghệ thông tin, internet, thư điện tử và các hệ thống thông tin của nhà trường một cách an toàn, đúng quy định; Khuyến khích cán bộ, giáo viên, nhân viên chủ động cập nhật kiến thức, kỹ năng phòng tránh các nguy cơ mất an toàn thông tin mạng.

Chương III
TRÁCH NHIỆM BẢO ĐẢM AN NINH MẠNG, AN TOÀN THÔNG TIN

Điều 12. Trách nhiệm của các bộ phận và cá nhân trong nhà trường

1. Các tổ chuyên môn, bộ phận và cá nhân trong nhà trường có trách nhiệm thực hiện các quy định tại Quy chế này và chịu trách nhiệm trước Hiệu trưởng trong công tác bảo đảm an ninh mạng, an toàn thông tin thuộc phạm vi quản lý.

2. Thường xuyên tuyên truyền, quán triệt các quy định về an ninh mạng, an toàn thông tin đến cán bộ, giáo viên, nhân viên trong nhà trường; nâng cao ý thức trách nhiệm trong việc sử dụng hệ thống thông tin và thiết bị công nghệ thông tin.

3. Phối hợp cung cấp thông tin và tạo điều kiện cho cơ quan có thẩm quyền hoặc đơn vị chuyên môn khi triển khai kiểm tra, đánh giá, khắc phục sự cố về an ninh mạng, an toàn thông tin.

4. Phối hợp chặt chẽ với các đơn vị liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an ninh mạng, an toàn thông tin.

5. Tổ trưởng tổ văn phòng phụ trách công nghệ thông tin của nhà trường có trách nhiệm:

- Tham mưu Hiệu trưởng triển khai các biện pháp bảo đảm an ninh mạng, an toàn thông tin trong nhà trường.

- Quản lý, vận hành và bảo vệ hệ thống thông tin theo quy định của pháp luật và Quy chế này.

- Kịp thời báo cáo Hiệu trưởng khi phát hiện sự cố an ninh mạng, mất an toàn thông tin và phối hợp với các cơ quan, đơn vị liên quan để xử lý.

Điều 13. Trách nhiệm của cán bộ, giáo viên, nhân viên và người lao động

1. Cán bộ, giáo viên, nhân viên và người lao động trong nhà trường có trách nhiệm:

a) Chấp hành Quy chế này và các quy định của pháp luật về an ninh mạng, an toàn thông tin; chịu trách nhiệm bảo đảm an toàn thông tin trong phạm vi nhiệm vụ được giao.

b) Tự quản lý, bảo quản và sử dụng an toàn tài khoản, thiết bị công nghệ thông tin được giao; không tự ý cài đặt phần mềm không rõ nguồn gốc hoặc làm ảnh hưởng đến an toàn hệ thống thông tin của nhà trường.

c) Khi phát hiện dấu hiệu mất an ninh mạng, mất an toàn thông tin, phải kịp thời báo cáo với Hiệu trưởng hoặc cán bộ phụ trách công nghệ thông tin để xử lý.

d) Tham gia đầy đủ các chương trình tập huấn, bồi dưỡng về an ninh mạng và an toàn thông tin do nhà trường hoặc cơ quan có thẩm quyền tổ chức.

2. Trách nhiệm của Tổ trưởng tổ văn phòng phụ trách công nghệ thông tin/an toàn thông tin

Ngoài các quy định tại Khoản 1 Điều này, Tổ trưởng tổ văn phòng phụ trách công nghệ thông tin/an toàn thông tin của nhà trường có trách nhiệm:

a) Tham mưu Hiệu trưởng triển khai thực hiện các quy định của Quy chế này và các quy định của pháp luật về an ninh mạng, an toàn thông tin.

b) Đề xuất ban hành hoặc thực hiện các biện pháp quản lý và giải pháp kỹ thuật nhằm bảo đảm an ninh mạng, an toàn thông tin trong nhà trường.

c) Quản lý, vận hành và bảo đảm an toàn cho hạ tầng kỹ thuật, thiết bị và hệ thống thông tin của nhà trường; hướng dẫn cán bộ, giáo viên, nhân viên thực hiện các quy định về an toàn thông tin khi sử dụng công nghệ thông tin.

d) Theo dõi, giám sát hoạt động của hệ thống thông tin; kịp thời báo cáo Hiệu trưởng khi xảy ra sự cố an ninh mạng hoặc mất an toàn thông tin để có biện pháp xử lý.

đ) Phối hợp với các bộ phận, cá nhân liên quan và cơ quan có thẩm quyền trong việc phát hiện, xử lý và khắc phục các sự cố an ninh mạng, an toàn thông tin.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 14. Kinh phí thực hiện

Kinh phí bảo đảm an ninh mạng, an toàn thông tin của nhà trường được bố trí từ nguồn ngân sách nhà nước theo quy định hiện hành. Kinh phí này được sử dụng để phục vụ các hoạt động như: duy trì, nâng cấp hệ thống công nghệ thông tin, bảo đảm an toàn thông tin, đào tạo, tập huấn và triển khai các biện pháp bảo vệ hệ thống thông tin của nhà trường theo quy định của pháp luật.

Điều 15. Chế độ, nội dung báo cáo, khen thưởng, kỷ luật

1. Tổ trưởng tổ văn phòng phụ trách công nghệ thông tin của nhà trường có trách nhiệm tham mưu Hiệu trưởng theo dõi, tổng hợp và báo cáo tình hình bảo đảm an ninh mạng, an toàn thông tin theo yêu cầu của cơ quan quản lý cấp trên.

2. Hằng năm, căn cứ kết quả thực hiện công tác bảo đảm an ninh mạng, an toàn thông tin, nhà trường xem xét biểu dương, khen thưởng các cá nhân có thành tích tốt theo quy định hiện hành.

3. Các cá nhân vi phạm quy chế này tùy theo tính chất, mức độ vi phạm sẽ bị xử lý theo quy định của pháp luật và quy định của nhà trường.

Điều 16. Công tác kiểm tra

Nhà trường và các bộ phận liên quan có trách nhiệm thường xuyên kiểm tra, theo dõi và đánh giá việc thực hiện công tác bảo đảm an ninh mạng, an toàn thông tin theo quy định. Công tác bảo đảm an ninh mạng, an toàn thông tin được xác định là một trong

những nhiệm vụ quan trọng trong hoạt động ứng dụng công nghệ thông tin của nhà trường.

Điều 17. Tổ chức thực hiện

1. Tổ trưởng tổ văn phòng, các tổ chuyên môn trong nhà trường có trách nhiệm triển khai, phổ biến và thực hiện nghiêm túc Quy chế này; thường xuyên kiểm tra việc thực hiện; chịu trách nhiệm trước Hiệu trưởng và trước pháp luật về việc bảo đảm an ninh mạng, an toàn thông tin trong phạm vi quản lý.

2. Tổ trưởng tổ văn phòng phụ trách công nghệ thông tin của nhà trường có trách nhiệm theo dõi, đôn đốc và kiểm tra việc thực hiện Quy chế; tham mưu Hiệu trưởng tổng hợp, báo cáo tình hình bảo đảm an ninh mạng, an toàn thông tin theo yêu cầu của cơ quan quản lý cấp trên.

Điều 18. Sửa đổi, bổ sung Quy chế

Trong quá trình thực hiện Quy chế này, nếu có khó khăn, vướng mắc hoặc cần sửa đổi, bổ sung, các tổ bộ phận và cá nhân trong nhà trường kịp thời báo cáo Hiệu trưởng để xem xét, quyết định điều chỉnh cho phù hợp.