SỞ GIÁO DỤC VÀ ĐÀO TẠO GIA LAI
TRƯỜNG THPT CHUYÊN LÊ QUÝ ĐÔN

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

Số: 102 /QĐ-CLQĐ

Quy Nhơn, ngày 01 tháng 11 năm 2025

QUYẾT ĐỊNH
V/v ban hành Quy chế đảm bảo an toàn, an ninh thông tin trong quản lý và dạy học của trường THPT chuyên Lê Quý Đôn từ năm học 2025-2026

HIỆU TRƯỞNG TRƯỜNG THPT CHUYÊN LÊ QUÝ ĐÔN

Căn cứ nhiệm vụ và quyền của Hiệu trưởng quy định tại Điều 11 của Điều lệ trường THCS, trường THPT và trường phổ thông có nhiều cấp học, ban hành kèm theo Thông tư số 32/2020/TT-BGDĐT ngày 15/9/2020 của Bộ GDĐT;

Căn cứ Quyết định số 3806/QĐ-BGDĐT ngày 29/11/2024 của Bộ trưởng Bộ GDĐT về việc ban hành Quy chế đảm bảo an toàn thông tin mạng của Bộ GDĐT;

Căn cứ Quyết định số 2475/QĐ-BGDĐT ngày 30/12/2022 của Bộ GDĐT Ban hành Bộ tiêu chí đánh giá mức độ CĐS của cơ sở giáo dục phổ thông và giáo dục thường xuyên;

Căn cứ Công văn số 2089/SGDĐT-VP ngày 21/10/2025 của Sở GDĐT Gia Lai v/v triển khai công tác bảo đảm an ninh mạng, an toàn thông tin của Sở GDĐT.

QUYẾT ĐỊNH:

Điều 1. Ban hành Quy chế đảm bảo an toàn, an ninh thông tin trong quản lý và dạy học của Trường THPT chuyên Lê Quý Đôn từ năm học 2025-2026.

Điều 2. Quy chế này được thông qua tại kì họp Hội đồng, website của nhà trường và có hiệu lực thi hành kể từ ngày ký. Quy chế sẽ được bổ sung sửa đổi khi có vấn đề mới nảy sinh hoặc không còn phù hợp và được thông báo bằng văn bản.

Điều 3. Phó Hiệu trưởng, tổ trưởng chuyên môn, phụ trách các bộ phận công tác viên chức, nhân viên, học sinh trong nhà trường chịu trách nhiệm thi hành quyết định này./.

Nơi nhận:
- Như điều 3;
- Lưu: VT.

HIỆU TRƯỞNG

SỞ GIÁO DỤC VÀ ĐÀO TẠO TỈNH GIA LAI
TRƯỜNG THPT CHUYÊN LÊ QUÝ ĐÔN

Huỳnh Lê Minh

SỞ GIÁO DỤC VÀ ĐÀO TẠO GIA LAI
TRƯỜNG THPT CHUYÊN LÊ QUÝ ĐÔN

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

QUY CHẾ
Quy chế bảo đảm an toàn, an ninh thông tin trong quản lý và dạy học của Trường THPT chuyên Lê Quý Đôn từ năm học 2025 - 2026

(Kèm theo Quyết định số: 102/QĐ-CLQĐ ngày 01 tháng 11 năm 2025 của Hiệu trưởng Trường THPT chuyên Lê Quý Đôn)

Chương I
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, anh ninh thông tin mạng trong hoạt động ứng dụng công nghệ thông tin (quản lý và dạy học) của Trường THPT chuyên Lê Quý Đôn (sau đây gọi tắt là trường).

2. Đối tượng áp dụng

Quy chế này áp dụng đối toàn bộ cán bộ, giáo viên, nhân viên và học sinh tham gia vận hành, khai thác các hệ thống thông tin của trường.

3. Mục đích đảm bảo an toàn, an ninh thông tin

Giảm thiểu được các nguy cơ gây sự cố mất an toàn, an ninh thông tin và đảm bảo an toàn về dữ liệu, các thiết bị công nghệ thông tin trong hoạt động ứng dụng công nghệ thông tin của Trường.

Điều 2. Giải thích từ ngữ

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

1. Mạng: khái niệm chỉ mạng viễn thông cố định, di động, Internet và mạng máy tính.

2. Tài khoản: bao gồm tên tài khoản và mật khẩu của người sử dụng.

3. Hệ thống thông tin: tập hợp thiết bị 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.

4. An toàn thông tin: sự bảo vệ thông tin và hệ thống thông tin 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.

5. Phần mềm độc hại: phần mềm có khả năng gây ra hoạt động không

bình thường cho một phần hoặc 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.

6. Người sử dụng: cán bộ, viên chức và người lao động.

7. LogFile: một tập tin được tạo ra bởi một máy chủ web hoặc máy chủ proxy có chứa tất cả thông tin về các hoạt động trên máy chủ đó, như thông tin người truy cập, thời gian khách viếng thăm, địa chỉ IP....

8. Cán bộ quản trị mạng: nhân viên CNTT, cán bộ được giao phụ trách công tác đảm bảo hạ tầng, ứng dụng, cơ sở dữ liệu và an toàn, an ninh thông tin cho việc triển khai, vận hành, khai thác hệ thống CNTT tại trường.

Điều 3. Phạm vi đảm bảo an toàn thông tin

1. Hệ thống phòng máy.

2. Hệ thống mạng.

3. 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.

4. Trang thiết bị công nghệ thông tin cá nhân.

Điều 4. Nguyên tắc đảm bảo an toàn thông tin mạng

1. 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 (dừng hoạt động) 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 tháng 7 năm 2016 của Chính phủ.

2. Bảo đảm an toàn thông tin mạng được thực hiện xuyên suốt, toàn bộ quá trình trong khâu thiết kế, xây dựng, mua sắm, nâng cấp, vận hành, bảo trì và ngừng sử dụng hạ tầng, hệ thống thông tin, phần mềm, dữ liệu.

3. Trách nhiệm bảo đảm an toàn thông tin mạng gắn với trách nhiệm của người đứng đầu cơ quan, đơn vị và cá nhân trực tiếp liên quan.

4. Trường hợp có văn bản, quy định cập nhật, thay thế hoặc quy định khác tại văn bản quy phạm pháp luật, quyết định của cấp có thẩm quyền cao hơn thì áp dụng quy định tại văn bản đó.

5. Thông tin thuộc Danh mục bí mật nhà nước được bảo vệ theo quy định của pháp luật về bảo vệ bí mật nhà nước.

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

Điều 5. Các hành vi bị nghiêm cấm

1. 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.

2. 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.

3. 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.

4. Phát tán thư rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo.

5. Thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác; lợi dụng sơ hở, điểm yếu của hệ thống thông tin để thu thập, khai thác thông tin cá nhân.

6. Xâm nhập trái pháp luật bí mật mật mã và thông tin đã mã hóa hợp pháp của cơ quan, tổ chức, cá nhân; tiết lộ thông tin về sản phẩm mật mã dân sự, thông tin về khách hàng sử dụng hợp pháp sản phẩm mật mã dân sự; sử dụng, kinh doanh các sản phẩm mật mã dân sự không rõ nguồn gốc.

7. Các hành vi bị nghiêm cấm quy định tại Điều 8 Luật An ninh mạng.

Chương II
BIỆN PHÁP BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 6. Các biện pháp quản lý kỹ thuật cơ bản trong công tác bảo đảm an toàn thông tin

1. 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. 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 chức năng, cổng giao tiếp mạng, giao thức và các dịch vụ không cần thiết.

2. Quản lý hệ thống mạng không dây (Wireless LAN): khi thiết lập mạng không dây, cần thiết lập các thông số an toàn và định kỳ ít nhất 3 tháng thay đổi mật khẩu truy cập nhằm tăng cường công tác bảo mật.

3. Tổ chức quản lý tài khoản: tiến hành rà soát ít nhất 6 tháng một lần các tài khoản và định danh người dùng trong hệ thống thông tin. Hủy tài khoản, quyền truy nhập hệ thống thông tin, thu hồi lại tất cả các tài sản liên quan tới hệ thống thông tin (khóa, thẻ nhận dạng, thư mục lưu trữ,...) đối với người sử dụng

không còn công tác hoặc không còn sử dụng do được cấp tài khoản mới.

4. Quản lý đăng nhập hệ thống: các hệ thống thông tin cần giới hạn số lần đăng nhập vào hệ thống, tự động khóa tài khoản khi liên tục đăng nhập sai vượt quá số lần quy định. Tổ chức theo dõi, giám sát tất cả các phương pháp đăng nhập từ xa, nhất là các trường hợp đăng nhập vào hệ thống với mục đích quản trị. Tăng cường việc sử dụng mạng riêng ảo (VPN - Virtual Private Network) khi có nhu cầu làm việc từ xa; yêu cầu người sử dụng đặt mật khẩu với độ an toàn cao.

5. Quản lý nhật ký sự kiện (Log File): hệ thống thông tin cần ghi nhận các sự kiện: Quá trình đăng nhập hệ thống, các thao tác cấu hình hệ thống, quá trình truy xuất hệ thống ... Thường xuyên kiểm tra, sao lưu (backup) các nhật ký sự kiện theo từng tháng để theo dõi, xác định những sự kiện đã xảy ra của hệ thống và hạn chế việc tràn nhật ký sự kiện gây ảnh hưởng đến hoạt động của hệ thống.

6. Chống phần mềm độc hại: triển khai các phần mềm chống mã độc trên các máy tính, thiết bị di động trong mạng để phát hiện, loại trừ phần mềm độc hại. Thường xuyên cập nhật các phiên bản mới, các bản vá lỗi của các phần mềm chống virus để bảo đảm chương trình quét virus của cơ quan trên các máy chủ, máy trạm luôn được cập nhật mới nhất; thiết lập chế độ quét thường xuyên ít nhất tuần 01 lần. Thường xuyên cập nhật bản vá các lỗ hổng bảo mật của hệ điều hành và các phần mềm ứng dụng trên máy tính để hạn chế tối đa rủi ro mất an toàn thông tin.

7. Bảo đảm an toàn cho Trang thông tin điện tử: thực hiện theo hướng dẫn tại Công văn số 2132/BTTTT-VNCERT ngày 18 tháng 7 năm 2011 của Bộ Thông tin và Truyền thông về việc hướng dẫn đảm bảo an toàn thông tin cho các Trang thông tin điện tử.

8. Thiết lập cơ chế sao lưu và phục hồi cho máy chủ, máy trạm: máy chủ và máy trạm cần được thực hiện các biện pháp sao lưu dữ liệu, thông tin quan trọng nhằm phục vụ cho công tác phục hồi dữ liệu một cách nhanh nhất.

9. Xử lý khẩn cấp: khi phát hiện hệ thống thông tin bị tấn công cần thực hiện các bước cơ bản sau:

Bước 1: Ngắt kết nối máy chủ ra khỏi mạng;

Bước 2: Sao chép nhật ký sự kiện và toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ (phục vụ cho hoạt động phân tích, điều tra);

Bước 3: Khôi phục hệ thống bằng cách chuyển dữ liệu sao lưu mới nhất để hệ thống hoạt động trở lại;

Bước 4: Chủ trì, phối hợp với các cơ quan liên quan thành lập đoàn kiểm tra an toàn thông tin định kỳ hàng năm hoặc kiểm tra đột xuất khi phát hiện có

các dấu hiệu vi phạm an toàn thông tin.

Điều 7. Các biện pháp quản lý vận hành trong công tác bảo đảm an toàn thông tin

1. Đối với cán bộ chuyên trách Công nghệ thông tin (CNTT)

a) Triển khai, thực hiện các nội dung của Điều 6 Quy chế này.

b) Nắm vững và thực hiện nghiêm túc các quy định về bảo vệ bí mật Nhà nước. Thường xuyên tự cập nhật các kiến thức về an toàn thông tin, nguy cơ tiềm ẩn có thể gây mất thông tin và các biện pháp phòng tránh khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ.

c) Phối hợp chặt chẽ với cơ quan Công an trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn, an ninh thông tin.

2. Đối với người sử dụng

a) Thường xuyên cập nhật những chính sách, quy trình, thủ tục an toàn thông tin của đơn vị cũng như thực hiện những hướng dẫn về an toàn thông tin của cán bộ chuyên trách công nghệ thông tin.

b) 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 thực hiện việc thu hồi chức năng này khi đã sử dụng xong.

c) Các tài khoản đăng nhập hệ điều hành cần phải đặt mật khẩu, khi không sử dụng thì phải khóa tài khoản.

Chương III
QUY ĐỊNH BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 8. Đảm bảo an toàn thông tin Hệ thống Phòng máy

1. Cán bộ quản trị mạng, nhân viên CNTT quản lý, vận hành hệ thống phòng máy của trường.

2. Phòng máy là khu vực hạn chế tiếp cận; chỉ những cá nhân có quyền, nhiệm vụ theo quy định mới được phép vào phòng máy.

Điều 9. Đảm bảo an toàn thông tin Hệ thống mạng

1. Cán bộ quản trị mạng, nhân viên CNTT quản lý, vận hành mạng nội bộ và dịch vụ Internet của trường; triển khai biện pháp kỹ thuật giám sát kết nối mạng Internet của thiết bị đầu cuối, phát hiện và ngăn chặn các hành vi xâm nhập từ mạng Internet.

2. Khi phát hiện nguy cơ mất an toàn thông tin (cảnh báo từ phần mềm phòng chống mã độc, máy tính hoạt động chậm bất thường, mất dữ liệu), đơn vị và cá nhân phải tắt thiết bị công nghệ thông tin, kịp thời thông báo với cơ quan

chức năng để được hỗ trợ xử lý.

Điều 10. Đảm bảo an toàn thông tin đối với các Hệ thống thông tin quản lý và cơ sở dữ liệu của trường

1. Đảm bảo an toàn thông tin trong xây dựng, nâng cấp hệ thống thông tin và cơ sở dữ liệu

a) Khi sử dụng hệ thống mới hoặc nâng cấp hệ thống thông tin, đơn vị quản lý hệ thống thông tin có trách nhiệm xây dựng phương án bảo đảm an toàn cho các hệ thống thông tin; rà soát cấp độ an toàn của hệ thống thông tin và thực hiện điều chỉnh, bổ sung hoặc thay mới hồ sơ đề xuất cấp độ trong trường hợp cần thiết.

b) Quá trình tổ chức xây dựng, nâng cấp hệ thống thông tin phải tuân thủ phương án bảo đảm an toàn thông tin đã đề xuất và theo các quy định của quản lý dự án công nghệ thông tin của Chính phủ.

2. Đảm bảo an toàn thông tin khi đưa vào khai thác sử dụng hệ thống thông tin và cơ sở dữ liệu

a) Đảm bảo an toàn thông tin trong quản lý, vận hành hệ thống thông tin

Các đơn vị vận hành hệ thống thông tin chịu trách nhiệm đảm bảo an toàn thông tin cho các hệ thống thông tin theo quy định tại các Điều 22, 23 và 24 của Luật An toàn thông tin mạng năm 2015.

Cán bộ quản trị mạng, nhân viên CNTT chịu trách nhiệm đảm bảo an toàn thông tin cho các hệ thống thông tin dùng chung của trường và chọn phương án bảo đảm an toàn cho các hệ thống thông tin. Thường xuyên kiểm tra, giám sát an toàn hệ thống thông tin; tuân thủ quy trình vận hành, quy trình xử lý sự cố đã xây dựng; lưu trữ đầy đủ thông tin nhật ký hệ thống thông tin để phục vụ quản lý và kiểm soát thông tin.

b) Đảm bảo an toàn thông tin trong quản lý và sử dụng tài khoản truy cập các hệ thống thông tin

Khi được cấp tài khoản sử dụng hệ thống thông tin, cá nhân phải đổi mật khẩu trong lần đăng nhập đầu tiên. Đặt mật khẩu có độ dài ít nhất 8 ký tự, gồm: chữ cái hoa và thường, chữ số và ký tự đặc biệt; thay đổi mật khẩu tối thiểu 01 lần/6 tháng. Cá nhân có trách nhiệm bảo mật thông tin tài khoản truy nhập, không chia sẻ mật khẩu với người khác. Đăng xuất hệ thống thông tin khi không sử dụng.

Cá nhân thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ hưu tạm khóa quyền truy cập tài khoản người sử dụng. Cán bộ quản trị mạng, nhân viên CNTT phải thông báo cho đơn vị vận hành hệ thống thông tin thực hiện điều chỉnh, tạm khóa, thu hồi hoặc hủy bỏ tài khoản.

Cán bộ quản trị mạng, nhân viên CNTT có quyền khóa quyền truy cập của tài khoản trong trường hợp tài khoản đó thực hiện các hành vi tấn công hoặc để xảy ra vấn đề mất an toàn thông tin.

Điều 11. Đảm bảo an toàn thông tin trang thiết bị công nghệ thông tin cá nhân

1. Cá nhân chịu trách nhiệm về đảm bảo an toàn thông tin thiết bị do mình quản lý và sử dụng.

2. Các thiết bị công nghệ thông tin cá nhân phải được cài đặt và cập nhật thường xuyên phần mềm phòng chống mã độc; thực hiện kiểm tra, rà quét bằng phần mềm phòng chống mã độc khi sao chép, mở các tập tin hoặc trước khi kết nối các thiết bị lưu trữ dữ liệu di động với máy tính của mình.

3. Cá nhân chịu trách nhiệm và có biện pháp đảm bảo an toàn thông tin, tránh bị lộ lọt dữ liệu khi thực hiện bảo hành, bảo dưỡng, sửa chữa hoặc bảo trì thiết bị do mình quản lý.

4. Khi ngừng sử dụng thiết bị công nghệ thông tin cá nhân, cá nhân phải thực hiện tiêu hủy dữ liệu theo quy định.

Điều 12. Bảo vệ bí mật nhà nước trong hoạt động ứng dụng công nghệ thông tin

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

a) Không được sử dụng máy tính nối mạng internet để soạn thảo văn bản, chuyển giao, lưu trữ thông tin có nội dung thuộc bí mật nhà nước; cung cấp tin, tài liệu và đưa thông tin bí mật nhà nước trên Cổng/Trang thông tin điện tử.

b) Không được in, sao chụp tài liệu bí mật nhà nước trên các thiết bị kết nối mạng internet.

2. Khi sửa chữa, khắc phục các sự cố của máy tính dùng soạn thảo văn bản mật, các bộ phận phải báo cáo cho người có thẩm quyền. Không được cho phép các công ty tư nhân hoặc người không có trách nhiệm trực tiếp sửa chữa, xử lý, khắc phục sự cố.

Trước khi thanh lý các máy tính trong đơn vị, cán bộ chuyên trách công nghệ thông tin phải dùng các biện pháp kỹ thuật xoá bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính.

Điều 13. Quy định về cấp phát, thu hồi, cập nhật và quản lý các tài khoản truy cập vào hệ thống thông tin

1. Cán bộ quản trị mạng quản lý, cấp tài khoản cá nhân và phân quyền truy cập cho người sử dụng trên tất cả các máy trạm đặt tại các phòng, bộ phận. Trong trường hợp cần thiết có thể hủy tài khoản truy cập cá nhân và ngắt kết nối đối với các hành vi cố ý tấn công hoặc gây trở ngại cho mạng máy tính; hủy

quyền truy cập hệ thống thông tin đối với cán bộ, giáo viên, nhân viên nghỉ chế độ, chuyển công tác và đảm bảo khả năng vẫn truy nhập được vào các hồ sơ được tạo ra bởi cán bộ, giáo viên, nhân viên đó.

2. Hướng dẫn người sử dụng thay đổi mật khẩu ngay sau khi đăng nhập lần đầu tiên; bảo vệ thông tin của tài khoản theo quy định.

Điều 14. Cơ chế sao lưu dữ liệu

1. Cán bộ quản trị mạng phối hợp với các 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, máy chủ), phần mềm ứng dụng, cơ sở dữ liệu, tệp tin ghi nhật ký hệ 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.

2. 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 đảm bảo sẵn sàng cho việc sử dụng khi cần; việc kiểm tra, phục hồi hệ thống từ dữ liệu sao lưu tối thiểu 6 tháng một lần (hoặc khi có yêu cầu đột xuất).

Điều 15. Cơ chế thông tin, báo cáo và khắc phục sự cố an toàn, an ninh thông tin

1. Đối với người sử dụng

a) Thông tin, báo cáo kịp thời cho cán bộ quản trị mạng khi phát hiện các sự cố gây mất an toàn, an ninh thông tin mạng trong quá trình tham gia vào hệ thống thông tin.

b) Phối hợp tích cực trong suốt quá trình giải quyết và khắc phục sự cố.

2. Đối với nhân viên CNTT- quản trị mạng

a) Áp dụng mọi biện pháp để khắc phục và hạn chế thiệt hại do sự cố xảy ra, lập biên bản báo cáo hiệu trưởng nhà trường.

b) Cung cấp đầy đủ, chính xác, kịp thời những thông tin cần thiết; thực hiện theo đúng hướng dẫn và tạo điều kiện thuận lợi cho cơ quan chức năng (Công an,Trung tâm ứng cứu sự cố mạng, máy tính Việt Nam VNCert...) tham gia khắc phục sự cố.

Chương IV
KHEN THƯỞNG, XỬ LÝ VI PHẠM

Điều 16. Khen thưởng

Cán bộ, viên chức và người lao động thực hiện tốt Quy chế này sẽ được xem xét đánh giá khen thưởng.

Điều 17. Xử lý vi phạm

1. Cán bộ, viên chức và người lao động có hành vi vi phạm quy chế này thì tùy theo tính chất, mức độ vi phạm bị xử lý kỷ luật.

2. Nếu gây thiệt hại có tính chất nghiêm trọng thì phải bồi thường về vật chất và bị truy cứu trách nhiệm hình sự theo quy định của Pháp luật hiện hành.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 18. Trách nhiệm của Hiệu trưởng

1. Chịu trách nhiệm trước Sở Giáo dục và Đào tạo trong công tác đảm bảo an toàn hệ thống thông tin của trường.

2. Khi có sự cố hoặc nguy cơ mất an toàn thông tin, kịp thời sử dụng cán bộ chuyên trách về an toàn, an ninh thông tin của đơn vị, áp dụng mọi biện pháp kỹ thuật để khắc phục, hạn chế thấp nhất mức thiệt hại có thể xảy ra.

3. Tạo điều kiện thuận lợi cho các cơ quan chức năng tham gia khắc phục sự cố và thực hiện đúng theo hướng dẫn.

4. Phân công cán bộ chuyên trách về an toàn hệ thống thông tin, đảm bảo an ninh thông tin, bảo mật trước khi tiến hành các hoạt động quản lý, vận hành hệ thống thông tin. Tạo điều kiện cho cán bộ chuyên trách được học tập, tiếp thu công nghệ và kiến thức về an toàn bảo mật thông tin.

5. Tổng hợp tình hình an toàn, an ninh thông tin và bảo mật của hệ thống thông tin theo định kỳ hàng năm để tổng hợp báo cáo Sở Giáo dục và Đào tạo.

Điều 19. Trách nhiệm của các Tổ trưởng

1. Phổ biến, tổ chức triển khai thực hiện tốt các quy định tại quy chế này đối với toàn thể công chức, viên chức và người lao động trong tổ.

2. Khi gặp sự cố cần phối hợp với nhân viên CNTT, cán bộ phụ trách mạng cung cấp thông tin và tạo điều kiện cho các đơn vị có chức năng triển khai công tác kiểm tra khắc phục kịp thời, nhanh chóng và đạt hiệu quả.

Điều 20. Trách nhiệm của Người sử dụng

1. Nghiêm chỉnh chấp hành các quy định, quy trình về an toàn, an ninh thông tin của nhà trường cũng như quy định khác của pháp luật, nâng cao ý thức cảnh giác và trách nhiệm bảo đảm an toàn, an ninh thông tin tại đơn vị.

2. Khi phát hiện sự cố phải báo ngay với Hiệu trưởng và cán bộ quản trị

mạng để kịp thời ngăn chặn, xử lý.

3. Hưởng ứng, tham gia các chương trình đào tạo, hội nghị về an toàn, an ninh thông tin do cơ quan chức năng tổ chức (nếu có).

4. Có trách nhiệm quản lý, bảo quản thiết bị được giao sử dụng; không tự ý thay đổi cấu hình hoặc tháo lắp các thiết bị trên máy tính khi chưa có sự đồng ý của Hiệu trưởng.

Điều 21. Trách nhiệm của cán bộ quản trị mạng

1. Cán bộ quản trị mạng: do Hiệu trưởng trường phân công, chịu trách nhiệm quản lý, vận hành các hoạt động hệ thống mạng máy tính. Tham mưu cho Hiệu trưởng trong việc đầu tư thiết bị phần cứng, phần mềm, công tác bảo mật thông tin trên môi trường mạng; sử dụng phần mềm có bản quyền và phần mềm mã nguồn mở cho hệ thống máy tính; cập nhật cấu hình chuẩn cho các thành phần của hệ thống khi tiến hành cài đặt và thiết lập cấu hình chặt chẽ nhất cho các sản phẩm an toàn thông tin nhưng vẫn duy trì yêu cầu hoạt động của hệ thống thông tin.

2. Sao chép, lưu trữ thông tin tại nơi an toàn; kiểm tra thông tin sao lưu để đảm bảo tính sẵn sàng và toàn vẹn của thông tin. Xử lý các sự cố về an toàn, an ninh thông tin và bảo mật hệ thống thông tin.

3. Triển khai các biện pháp chống virus, thư rác cho hệ thống máy chủ và tại các máy trạm, các thiết bị di động. Sử dụng biện pháp chống virus, thư rác để phát hiện và loại trừ những đoạn mã độc (virus, trojan.,.) được truyền tải bởi: thư điện tử, tập tin đính kèm từ Internet, thiết bị lưu trữ tháo lắp để khai thác lỗ hổng của hệ thống thông tin, Thường xuyên cập nhật các phần mềm chống virus, thư rác, bản vá lỗi hệ thống và hướng dẫn người dùng (user) sử dụng chương trình để bảo vệ an toàn dữ liệu.

4. Theo dõi và quản lý hoạt động hệ thống mạng, đề xuất lựa chọn công nghệ và triển khai các giải pháp nhằm đảm bảo cho hệ thống mạng cục bộ (LAN) hoạt động thông suốt, đảm bảo an toàn và bảo mật các thông tin truyền dẫn cho hệ thống mạng máy tính và đảm bảo hệ thống mạng LAN luôn được kết nối, hoạt động thông suốt.

5. Xây dựng quy trình, thử nghiệm, trực tiếp cài đặt, quản lý các phần mềm hệ thống và phần mềm ứng dụng trong hệ thống mạng máy tính; nghiên cứu, đề xuất, nâng cấp công nghệ phần mềm theo định hướng quản lý Nhà nước của ngành và tuân theo quy định của Chính phủ. Lắp đặt, hướng dẫn sử dụng, nâng cấp, cập nhật, bảo trì và quản trị mạng máy tính đảm bảo hoạt động ổn định và an toàn cho người sử dụng. Kiểm tra và xử lý các lỗi kỹ thuật đảm bảo việc truyền, nhận thông tin thông suốt trong giáo viên. Giữ bí mật tuyệt đối các thông tin trên mạng.

6. Thực hiện việc đánh giá, báo cáo và đề xuất với Hiệu trưởng các biện pháp phòng chống các rủi ro và mức độ nghiêm trọng của rủi ro đối với hệ thống thông tin của cơ quan (các rủi ro có thể xảy ra do sự truy cập, sử dụng thông tin trái phép; mất thông tin; thay đổi hoặc phá hủy thông tin của hệ thống).

Điều 22. Chế độ báo cáo, kiểm tra định kỳ và đột xuất

1. Định kỳ hàng năm, Hiệu trưởng báo cáo tình hình an toàn, an ninh thông tin gửi Sở Giáo dục và Đào tạo theo quy định.

2. Phối hợp với các đơn vị có liên quan tiến hành kiểm tra công tác đảm bảo an toàn, an ninh thông tin mạng.

3. Phối hợp với đoàn kiểm tra tiến hành kiểm tra đột xuất các cá nhân có dấu hiệu vi phạm an toàn, an ninh thông tin.

Điều 23. Kinh phí thực hiện

1. Kinh phí đảm bảo ATTT mạng thực hiện lồng ghép, tích hợp với các chương trình, đề án, nhiệm vụ công nghệ thông tin từ nguồn ngân sách nhà nước và các nguồn kinh phí hợp pháp khác;

2. Kế toán xây dựng kế hoạch, đề xuất dự toán kinh phí cho các hoạt động đảm bảo an toàn thông tin mạng trình cấp cơ quan cấp trên thẩm định và phê duyệt.

Điều 24. Điều khoản thi hành

1. Hiệu trưởng có trách nhiệm phổ biến, quán triệt đến toàn bộ viên chức và người lao động trong đơn vị thực hiện các quy định của Quy chế này; thường xuyên kiểm tra việc thực hiện Quy chế này tại đơn vị; chịu trách nhiệm trước pháp luật và Lãnh đạo Sở Giáo dục và Đào tạo về các vi phạm, thất thoát thông tin, dữ liệu thuộc phạm vi quản lý của đơn vị, do không tổ chức, chỉ đạo và kiểm tra cán bộ của đơn vị thực hiện đúng Quy chế.

2. Trong quá trình thực hiện Quy chế này nếu phát hiện những vấn đề khó khăn, vướng mắc, những điều không phù hợp cần sửa đổi, bổ sung, các cá nhân kịp thời báo cáo về Tổ Văn phòng để tổng hợp trình Hiệu trưởng xem xét, điều chỉnh, bổ sung cho phù hợp./.
