

QUY CHẾ

**Đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin
của Trường Trung học cơ sở Quang Trung**

*(Ban hành kèm theo Quyết định số 330/QĐ-THCS.QT ngày 24/10/2022
Trường Trung học cơ sở Quang Trung)*

Chương I

NHỮNG QUY ĐỊNH CHUNG

Điều 1: Phạm vi điều chỉnh

Quy chế này quy định việc đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của Trường Trung học cơ sở Quang Trung.

Điều 2: Đối tượng áp dụng

Quy chế này được áp dụng đối với cán bộ, viên chức và người lao động thuộc Trường Trung học cơ sở Quang Trung trong việc quản lý, khai thác, sử dụng và đảm bảo an toàn, an ninh thông tin của nhà trường phục vụ công tác chuyên môn.

Điều 3: Giải thích từ ngữ

1. An toàn thông tin: bao gồm các hoạt động quản lý, nghiệp vụ và kỹ thuật đối với hệ thống thông tin nhằm bảo vệ, khôi phục các hệ thống và nội dung thông tin đối với nguy cơ tự nhiên hoặc do con người gây ra. An toàn thông tin bao hàm các nội dung bảo vệ và bảo mật thông tin, an toàn dữ liệu, an toàn máy tính và an toàn mạng.
2. Hệ thống thông tin: là một hệ thống bao gồm con người, dữ liệu, các quy trình và công nghệ thông tin tương tác với nhau để thu thập, xử lý, lưu trữ và cung cấp thông tin cần thiết nhằm hỗ trợ cho một hệ thống.
3. Tính toàn vẹn: bảo vệ tính chính xác và tính đầy đủ của thông tin và các phương pháp xử lý thông tin.
4. Tính tin cậy: đảm bảo thông tin chỉ có thể được truy cập bởi những người được cấp quyền sử dụng.
5. Tính sẵn sàng: đảm bảo những người được cấp quyền có thể truy cập thông tin và các tài nguyên (mạng, máy chủ, tên miền, tài khoản thư điện tử...) ngay khi có nhu cầu.
6. Người dùng: cán bộ, viên chức và người lao động nhà trường sử dụng máy tính, các thiết bị điện tử để xử lý công việc.
7. Tham số mạng: Là các tham số kỹ thuật được cài đặt trong các thiết bị mạng và thiết bị máy tính để tạo ra các địa chỉ kết nối trong mạng. Các máy tính gửi và nhận thông tin thông qua các địa chỉ kết nối này.

Chương II

TRÁCH NHIỆM QUẢN LÝ, SỬ DỤNG ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 4. Quản lý thiết bị công nghệ thông tin (CNTT)

1. Thiết bị CNTT được trang bị tại bộ phận chuyên môn là tài sản của Nhà nước, được quản lý, sử dụng theo quy định của nhà trường và của Nhà nước. Các cán bộ, viên chức và người lao động có trách nhiệm quản lý trang thiết bị được giao.

2. Giao cho Nhân viên Công nghệ thông tin, Văn phòng nhà trường làm công tác quản trị mạng, trực tiếp quản lý kỹ thuật và duy trì hoạt động của hệ thống thông tin của nhà trường; là đầu mối kết nối mạng Internet; kiểm tra hiện trạng, đề xuất sửa chữa hoặc mua mới các chủng loại thiết bị CNTT phù hợp, an toàn, bảo mật theo quy định về quản lý, sử dụng tài sản cơ quan.

Điều 5. Quản lý, khai thác, sử dụng cơ sở dữ liệu và phần mềm

1. Văn phòng nhà trường có trách nhiệm cài đặt, quản lý các phần mềm hệ thống và phần mềm ứng dụng trong hệ thống mạng máy tính tại nhà trường; 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 Nhà nước.

2. Toàn thể cán bộ, viên chức, người lao động có trách nhiệm phối hợp trong quá trình triển khai, khai thác và sử dụng phần mềm.

Điều 6. Phòng chống virus máy tính, bảo mật cơ sở dữ liệu và an ninh mạng

1. Bảo mật số liệu: Cán bộ, viên chức, người lao động phải có trách nhiệm bảo mật số liệu nghiệp vụ trên máy tính. Việc chia sẻ dữ liệu trên mạng do bộ phận quản trị mạng thực hiện theo quyết định của Hiệu trưởng nhà trường.

2. Bảo mật truy cập: Các chương trình ứng dụng, phân chia sử dụng trên máy tính phải được đặt mật khẩu, mã khoá bảo mật.

3. Bảo mật hệ thống mạng và truyền tin: Mạng và đường truyền được áp dụng các chế độ bảo mật cần thiết, chống xâm nhập bất hợp pháp. Bộ phận quản trị mạng có trách nhiệm thường xuyên theo dõi, kiểm tra phát hiện kịp thời các hoạt động xâm nhập và có biện pháp xử lý kịp thời.

4. An toàn trong sử dụng: Khi không làm việc với máy vi tính trong thời gian dài, cán bộ, viên chức, người lao động trong nhà trường phải tắt máy tính hoặc đặt chế độ bảo vệ để đảm bảo an toàn cho dữ liệu của cá nhân.

5. Phòng, chống virus: Cán bộ, viên chức, người lao động trong nhà trường có trách nhiệm tuân thủ các biện pháp phòng và chống virus cho máy tính, đảm bảo an toàn dữ liệu thuộc cá nhân quản lý. Mọi dữ liệu từ các thiết bị lưu trữ bên ngoài đều phải được quét, diệt virus mỗi khi đưa vào máy. Những máy tính phát hiện có virus phải được tách khỏi mạng về mặt vật lý để tránh tình trạng lây nhiễm sang các máy tính khác. Không truy cập vào các link liên kết không rõ

ràng; không click vào các link, tải về các file tài liệu từ các địa chỉ thư không nắm rõ thông tin, địa chỉ người gửi. Cài đặt phần mềm phòng và chống virus cho máy tính, đảm bảo an toàn dữ liệu của đơn vị.

Điều 7. Đảm bảo an toàn máy chủ các thiết bị di động và cơ chế sao lưu, phục hồi

1. Kiểm soát chặt chẽ việc cài đặt các phần mềm mới lên máy chủ và các thiết bị di động. Các phần mềm được cài đặt trên máy chủ và các thiết bị di động (bao gồm hệ điều hành, các phần mềm ứng dụng văn phòng, phần mềm phục vụ công việc, tiện ích khác) phải được thường xuyên theo dõi, cập nhật bản vá lỗi bảo mật của nhà phát triển, lựa chọn cài đặt các phần mềm chống, diệt virus, mã độc và thường xuyên cập nhật phiên bản mới, đặt lịch quét virus theo định kỳ.

2. Cơ chế sao lưu, phục hồi máy chủ:

Cán bộ, viên chức và người lao động phải sao lưu định kỳ cơ sở dữ liệu và các dữ liệu quan trọng khác (bao gồm dữ liệu phát sinh trong quá trình vận hành các phần mềm ứng dụng như: các tập tin văn bản, hình ảnh,...). Sau khi sao lưu, lưu trữ bản sao lưu bằng thiết bị lưu trữ ngoài theo quy định lưu trữ hiện hành nhằm phục vụ cho việc phục hồi, khắc phục hệ thống kịp thời khi có sự cố xảy ra.

Điều 8. Đảm bảo an toàn hệ thống mạng máy tính, kết nối Internet

1. Quản lý hệ thống mạng nội bộ: Mạng nội bộ của nhà trường phải được tổ chức theo mô hình Clients/Server; mạng nội bộ khi kết nối với mạng Internet phải thông qua thiết bị tường lửa kiểm soát, có phân chia hệ thống mạng nội bộ thành các vùng mạng theo phạm vi truy cập, vô hiệu hóa tất cả các dịch vụ không sử dụng tại từng vùng mạng, thực hiện nguyên tắc chỉ mở các dịch vụ cần thiết khi có yêu cầu.

2. Quản lý hệ thống mạng không dây (wifi): Khi thiết lập mạng không dây có kết nối vào mạng nội bộ phải thiết lập các thông số cần thiết như định danh, mật mã, mã hóa dữ liệu, có thay đổi mật mã định kỳ.

3. Quản lý truy cập từ xa vào mạng nội bộ: Đối với việc truy cập từ xa vào mạng nội bộ phải được theo dõi, quản lý chặt chẽ, nhất là truy cập có sử dụng chức năng quản trị, phải thiết lập mật mã độ an toàn cao, thường xuyên thay đổi mật mã, hạn chế truy cập từ xa vào mạng nội bộ từ các điểm truy cập Internet công cộng.

Điều 9. Đảm bảo an toàn truy cập, đăng nhập hệ thống thông tin

1. 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.

2. Mật mã đăng nhập, truy cập hệ thống thông tin phải có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số hoặc ký tự đặc biệt như !, @, #, \$, %, ...).

Điều 10. Đảm bảo an toàn thông tin, dữ liệu

1. Thông tin, dữ liệu khi được lưu trữ, khai thác, trao đổi phải được đảm bảo tính toàn vẹn, tính tin cậy, tính sẵn sàng. Thông tin, dữ liệu quan trọng khi được lưu trữ, trao đổi phải áp dụng kỹ thuật mã hóa, thiết lập mật mã, ứng dụng chữ ký số và phải có cơ chế lưu trữ dự phòng.

2. Trong trao đổi thông tin, dữ liệu phục vụ công việc, cơ quan, cán bộ, viên chức và người lao động phải sử dụng hệ thống thông tin chung của nhà trường quy định. Hạn chế việc sử dụng các phương tiện trao đổi thông tin dữ liệu, hệ thống thư điện tử công cộng, mạng xã hội trên Internet trong hoạt động của nhà trường.

Điều 11. Những điều không được làm

1. Không được lợi dụng việc sử dụng Internet nhằm mục đích: Chống lại nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội; kích động bạo lực, đòi truy, tệ nạn xã hội, mê tín dị đoan; phá hoại thuần phong mỹ tục của dân tộc...

2. Không được tiết lộ bí mật nhà nước và các bí mật khác đã được pháp luật quy định.

3. Không được tham gia, đăng tải những thông tin chưa xác minh, sai lệch và những nội dung liên quan đến đơn vị khi chưa được sự chấp thuận của Hiệu trưởng.

4. Không được chơi các trò chơi trực tuyến (game online) hoặc các trò chơi khác trên Internet trong giờ làm việc.

5. Không được truy cập hoặc tải các trang website có nội dung đồi trụy, phản động, các chương trình không rõ nguồn gốc, các thông tin quảng cáo hấp dẫn.

6. Không sử dụng thông tin của đơn vị sai mục đích, không cung cấp thông tin đơn vị (thông tin học sinh, nhân sự, dữ liệu hình ảnh camera, ...) cho đối tượng, đơn vị khác.

7. Khi sử dụng hệ thống thư điện tử (Email) không được kích chuột vào bất cứ thư điện tử, tệp đính kèm, đường link, thư rác, thư quảng cáo nào không rõ nguồn gốc và không xác định được người gửi.

Chương III TỔ CHỨC THỰC HIỆN

Điều 12. Điều khoản thi hành

1. Các cán bộ, viên chức và người lao động nhà trường có trách nhiệm thực hiện nghiêm túc Quy chế này.

2. Mọi hành vi vi phạm các điều khoản trong Quy chế, tùy theo tính chất, mức độ sẽ bị xử lý kỷ luật, xử phạt vi phạm hành chính, bồi thường vật chất, khắc phục hậu quả hoặc truy cứu trách nhiệm hình sự theo quy định của pháp luật hiện hành.

3. Trong quá trình thực hiện, nếu có vấn đề phát sinh hoặc khó khăn, vướng mắc cần phản ánh kịp thời về Văn phòng nhà trường tổng hợp báo cáo Hiệu trưởng, thông qua Hội đồng trường xem xét quyết định điều chỉnh, bổ sung cho phù hợp./.

HIỆU TRƯỞNG



Vũ Mai Hương

