SỞ GD&ĐT QUẢNG NGÃI
TRƯỜNG THPT SỐ 1 NGHĨA HÀNH

Số: 98 /QĐ-NH1

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

Nghĩa Hành, ngày 31 tháng 12 năm 2023

QUYẾT ĐỊNH
Ban hành Quy chế đảm bảo an toàn ứng dụng công nghệ thông tin và chuyển đổi số của trường THPT Số 1 Nghĩa Hành

HIỆU TRƯỞNG TRƯỜNG THPT SỐ 1 NGHĨA HÀNH

Căn cứ Quyết định số 131/QĐ-TTg ngày 25/01/2022 của Thủ tướng Chính phủ về phê duyệt Đề án "Tăng cường ứng dụng công nghệ thông tin và chuyển đổi số trong giáo dục và đào tạo giai đoạn 2022-2025, định hướng đến năm 2030";

Thực hiện Chỉ thị số 19-CT/TU ngày 18/5/2022 của Ban Thường vụ Tỉnh ủy về tăng cường sự lãnh đạo, chỉ đạo của Đảng đối với chuyển đổi số tỉnh Quảng Ngãi đến năm 2025, định hướng đến năm 2030, để tạo bước đột phá về phát triển chính quyền điện tử hướng đến chính quyền số, kinh tế số, xã hội số, góp phần nâng cao chất lượng cuộc sống của người dân, ngày 06/9/2023 Ban Thường vụ Tỉnh ủy ban hành Nghị Quyết số 13-NQ/TU về chuyển đổi số tỉnh Quảng Ngãi đến năm 2025, định hướng đến năm 2030.

Căn cứ chức năng, quyền hạn của Hiệu trưởng được quy định tại 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 GD và ĐT;

Theo đề nghị của bộ phận chuyển đổi số, an toàn thông tin,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế đảm bảo an toàn ứng dụng công nghệ thông tin và chuyển đổi số của trường THPT Số 1 Nghĩa Hành.

Điều 2. Quy chế này áp dụng cho tất cả các bộ phận, cá nhân, có liên quan đến việc sử dụng, quản lý và bảo vệ hệ thống công nghệ thông tin của trường, bao gồm: cán bộ, giáo viên, nhân viên và học sinh trong trường.

Điều 3. Viên chức phụ trách công nghệ thông tin có trách nhiệm hướng dẫn, giám sát và đánh giá việc thực hiện.

Điều 4. Quyết định này có hiệu lực kể từ ngày ký.

Điều 5. Các bộ phận, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- VP Sở GDĐT (báo cáo)
- HT; các PHT;
- CBGVNV toàn trường;
- Website trường;
- Lưu: VT, VP, bmp

HIỆU TRƯỞNG

Lê Văn Triều

QUY CHẾ
ĐẢM BẢO AN TOÀN ỨNG DỤNG CÔNG NGHỆ THÔNG TIN VÀ CHUYỂN ĐỔI SỐ CỦA TRƯỜNG THPT SỐ 1 NGHĨA HÀNH

(kèm theo Quyết định số 98 /QĐ-NH1 ngày 31/12/2023 của Hiệu trưởng trường THPT số 1 Nghĩa Hành)

Chương I. Quy định chung

Điều 1. Mục đích và yêu cầu

Quy chế này được xây dựng với mục đích bảo vệ hệ thống công nghệ thông tin, đảm bảo an toàn dữ liệu và bảo mật thông tin trong quá trình ứng dụng công nghệ thông tin và chuyển đổi số tại trường THPT Số 1 Nghĩa Hành.

Quy chế yêu cầu tất cả cán bộ, giáo viên, nhân viên và học sinh tuân thủ quy định về bảo mật thông tin, ngăn ngừa rủi ro về sự cố mạng, bảo vệ dữ liệu và đảm bảo sự ổn định của hệ thống công nghệ thông tin.

Điều 2. Phạm vi áp dụng

Quy chế này áp dụng đối với các hệ thống thông tin, cơ sở dữ liệu, phần mềm và các thiết bị liên quan đến công nghệ thông tin được sử dụng tại trường.

Quy chế cũng áp dụng cho quá trình chuyển đổi số, bao gồm việc triển khai các hệ thống phần mềm, các công cụ quản lý học tập và các dịch vụ công nghệ thông tin trong giảng dạy, học tập và quản lý hành chính.

Điều 3: Giải thích từ ngữ

1. An toàn thông tin là 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, các dịch vụ 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, phục vụ cho hoạt động lưu trữ, xử lý, truyền đưa, chia sẻ, trao đổi, cung cấp và sử dụng thông tin.

3. An ninh thông tin là việc bảo đảm thông tin trên mạng không gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

4. Sự cố an toàn thông tin mạng là việc thông tin, hệ thống thông tin bị tấn công hoặc gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng. Sự cố có thể là sự kiện đã, đang hoặc có khả năng xảy ra gây mất an toàn thông tin trên môi trường mạng (LAN, WAN, Internet,…), được phát hiện thông qua việc giám sát, đánh giá, phân tích của các cơ quan, tổ chức,

cá nhân có liên quan hoặc được cảnh báo từ các chuyên gia, tổ chức về lĩnh vực an toàn thông tin trong nước và trên thế giới.

5. 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.

6. Tính toàn vẹn là bảo vệ tính chính xác và tính đầy đủ của thông tin và các phương pháp xử lý thông tin.

7. Tính tin cậy là đảm bảo thông tin chỉ có thể được truy cập bởi những người được cấp quyền sử dụng.

8. Tính sẵn sàng là 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.

9. Người dùng là cán bộ, viên chức và người lao động sử dụng máy tính, các thiết bị điện tử để xử lý công việc.

10. 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. Các biện pháp đảm bảo an toàn thông tin

Điều 4. Quản lý thiết bị và bảo vệ dữ liệu

Thiết bị CNTT được trang bị tại trường là tài sản của Nhà nước, được quản lý, sử dụng theo Quy chế quản lý, sử dụng tài sản của đơn vị, quy định của Sở Giáo dục và Đào tạo, của Nhà nước. Các phòng, cán bộ, viên chức và người lao động có trách nhiệm quản lý trang thiết bị được giao.

Dữ liệu của trường THPT Số 1 Nghĩa Hành bao gồm thông tin học sinh, giáo viên, nhân viên, và các thông tin quản lý hành chính phải được bảo mật tuyệt đối, không để lộ lọt ra ngoài.

Mọi dữ liệu cần phải được sao lưu định kỳ, đảm bảo khả năng phục hồi khi có sự cố.

Điều 5. Đảm bảo an toàn hạ tầng công nghệ thông tin

Các thiết bị hạ tầng công nghệ thông tin như máy chủ, máy tính, thiết bị lưu trữ phải được quản lý, bảo trì định kỳ và được bảo vệ khỏi các cuộc tấn công mạng.

Các hệ thống và phần mềm phải được cập nhật bảo mật thường xuyên, tránh các lỗ hổng an ninh.

Điều 6. Quản lý truy cập

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

Tất cả người dùng hệ thống phải có quyền truy cập chỉ trong phạm vi công việc của mình.

Mật khẩu của người dùng phải tuân thủ các quy định về độ mạnh, mật khẩu 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 !, @, #, $, %,...). Không được chia sẻ mật khẩu cho người khác.

Điều 7. Phòng chống virus máy tính, bảo mật cơ sở dữ liệu và an ninh mạng

1. Bảo mật số liệu: Cán bộ, viên chức và 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 và theo phân cấp sử dụng tài nguyên mạng.

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 và người lao động 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 và người lao động có trách nhiệm tuân thủ các biện pháp phòng và chống virus cho máy tính, đảm bảo an toàn dữ liệu thuộc cá nhân được giao 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 đường link liên kết không rõ ràng; không mở các link, tải về các tập tin tài liệu từ các địa chỉ thư không nắm rõ thông tin, địa chỉ người gửi.

Điều 8. Đảm bảo an toàn máy chủ, máy trạm, 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, máy trạm và các thiết bị di động. Các phần mềm được cài đặt trên máy chủ, máy trạm 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, máy trạm: 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 9. Đảm bảo an toàn hệ thống mạng máy tính, kết nối Internet

1. Quản lý hệ thống mạng nội bộ: 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: 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.

Chương III. Phương án cơ bản đảm bảo an toàn thông tin

Điều 10. Chính sách an toàn thông tin

Xây dựng chính sách, quy trình quản lý, vận hành hoạt động bình thường của hệ thống nhằm bảo đảm tính sẵn sàng của hệ thống trong quá trình vận hành, khai thác.

1. Đảm bảo an toàn mức vật lý:

Hệ thống thiết bị mạng trung tâm được quản lý tập trung, có phòng riêng biệt, người có nhiệm vụ mới được phép vào trong.

Có hệ thống điện UPS dự phòng. Hệ thống chống sét cho toàn nhà, thiết bị chống sét nguồn điện.

2. Quản lý an toàn mạng:

Hệ thống mạng được thiết kế thống nhất, được quản lý định danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý và bảo đảm an toàn và bảo mật.

Hệ thống mạng nội bộ (LAN) được bảo vệ bằng tường lửa *(tích hợp tường lửa trên Router board nếu có)* và phân chia hệ thống mạng thành các vùng mạng quản lý theo chính sách an toàn thông tin riêng.

Mạng không dây, được đặt mật khẩu và theo định kỳ 3 tháng thay đổi mật khẩu truy cập nhằm tăng cường công tác bảo mật. Có cơ chế xác thực và mã hóa khi sử dụng mạng không dây.

3. Quản lý an toàn dữ liệu:

Có cơ chế thông báo để các bộ phận, các đoàn thể, các cá nhân lưu dữ liệu dự phòng, lưu trữ dữ liệu cá nhân ra thiết bị ngoại vi an toàn đồng thời thường xuyên kiểm tra để đảm bảo sẵn sàng phục hồi nhằm ngăn ngừa và hạn chế khi sự cố an toàn thông tin mạng xảy ra.

Thiết lập sao lưu cơ sở dữ liệu định kỳ trên máy chủ của nhà cung cấp dịch vụ công nghệ thông tin, nếu có.

Chỉ có Quản trị hệ thống mới có quyền truy cập phải được phân ra theo từng cấp độ tương ứng với từng nhiệm vụ của nhân viên và phải được phê duyệt từ cấp trên.

4. Quản lý an toàn người sử dụng đầu cuối:

Việc sử dụng các thiết bị lưu trữ ngoài như ổ cứng di động, các loại thẻ nhớ, thiết bị lưu trữ USB,... phải thường xuyên quét virus trước khi đọc hoặc sao chép dữ liệu.

Không sử dụng các máy tính thuộc sở hữu cá nhân (*máy xách tay của cá nhân, PDA*) hoặc những thiết bị lưu trữ di động cá nhân vào mục đích không phải nhiệm vụ. Hạn chế tối đa việc sử dụng các thiết bị lưu trữ ngoài để sao chép, di chuyển dữ liệu.

Các thiết bị đầu cuối khi kết nối phải được quản lý và cập nhật thông tin (*tên, chủng loại, địa chỉ MAC, địa chỉ IP*). Sử dụng cơ chế xác thực và sử dụng giao thức mạng an toàn.

Thường xuyên theo dõi, kiểm tra các lỗ hổng bảo mật và quản lý kết nối, truy cập khi sử dụng thiết bị đầu cuối từ xa.

Viên chức chuyên trách về an toàn thông tin thường xuyên theo dõi cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống đối với các cán bộ, công chức và người lao động đã nghỉ hưu, chuyển công tác, nghỉ việc.

Theo dõi cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho máy tính người sử dụng và thực hiện quy trình trước khi đưa hệ thống vào sử dụng.

Điều 11. Phối hợp với những cơ quan/tổ chức có thẩm quyền

Ban ứng dụng, an toàn thông tin chủ trì tham mưu lãnh đạo thực hiện nhiệm vụ phối hợp với Văn phòng Sở GDĐT, Sở Thông tin và Truyền thông và các đơn vị có liên quan tiến hành kiểm tra công tác bảo đảm an toàn thông tin mạng định kỳ hàng năm hoặc theo chỉ đạo của cấp có thẩm quyền đối với các cơ quan nhà nước trong tỉnh.

Điều 12. Quy định về quản lý an toàn dữ liệu

Thực hiện quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã kiểm tra tính nguyên vẹn.

Có cơ chế sao lưu dữ liệu dự phòng, lưu trữ dữ liệu tại nơi an toàn đồng thời thường xuyên kiểm tra để đảm bảo sẵn sàng phục hồi nhằm ngăn ngừa và hạn chế khi sự cố an toàn thông tin mạng xảy ra.

Tiến hành cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ được thực hiện theo yêu cầu của đơn vị vận hành hệ thống. Sử dụng mật mã để bảo đảm an toàn và bảo mật dữ liệu trong lưu trữ.

Quản lý chặt chẽ các thiết bị lưu trữ dữ liệu, nghiêm cấm việc di chuyển, thay đổi vị trí khi chưa được phép của người có thẩm quyền.

Quản lý và phân quyền truy cập phần mềm ứng dụng và cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ của người sử dụng. Quyền truy cập phải được phân ra theo từng cấp độ tương ứng với từng nhiệm vụ của cán bộ, viên chức, người lao động và phải được phê duyệt từ cấp trên.

Chương IV. Chuyển đổi số trong giáo dục

Điều 13. Mục tiêu chuyển đổi số

Phát triển các công cụ, phần mềm phục vụ cho việc giảng dạy và học tập trực tuyến, quản lý học sinh, điểm số và kết quả học tập.

Tạo ra một môi trường học tập, làm việc số hóa, tăng cường khả năng kết nối và quản lý hiệu quả.

Điều 14. Các biện pháp triển khai chuyển đổi số

Triển khai hệ thống học trực tuyến, lưu trữ tài liệu học tập và các hoạt động quản lý hành chính dưới dạng điện tử.

Đảm bảo an toàn thông tin cho các hoạt động học trực tuyến, bao gồm bảo mật thông tin học sinh và các tài liệu giảng dạy.

Chương V. Các quy định về kiểm tra, giám sát và xử lý vi phạm

Điều 15. Kiểm tra, giám sát

Phòng Công nghệ thông tin có trách nhiệm thực hiện kiểm tra, giám sát việc thực hiện quy chế này.

Định kỳ tổ chức đánh giá mức độ thực hiện an toàn thông tin và chuyển đổi số.

Điều 16. Xử lý vi phạm

Cán bộ, giáo viên, nhân viên, học sinh vi phạm các quy định về bảo mật thông tin và ứng dụng công nghệ thông tin sẽ bị xử lý theo quy định của trường.

Mức độ xử lý vi phạm sẽ tùy thuộc vào tính chất và mức độ của hành vi vi phạm.

Chương VI. Điều khoản thi hành

Điều 17. Quy chế này có hiệu lực từ ngày ký và được áp dụng cho tất cả các cá nhân, bộ phận liên quan tại trường THPT Số 1 Nghĩa Hành.

Điều 18. Các bộ phận, đoàn thể, cá nhân có trách nhiệm tổ chức thực hiện, giám sát và đánh giá hiệu quả thực hiện quy chế này./.