UBND TỈNH NGHỆ AN
**TRƯỜNG ĐHYK VINH**

Số: 1283 /QĐ-ĐHYKV

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

*Nghệ An, ngày 22 tháng 8 năm 2023*

# QUYẾT ĐỊNH

**Về việc ban hành quy định bảo đảm an toàn, an ninh mạng cho các hệ thống thông tin của Trường Đại học Y khoa Vinh**

## HIỆU TRƯỞNG TRƯỜNG ĐẠI HỌC Y KHOA VINH

*Căn cứ Luật An ninh mạng số24/2018/QH14 ngày 12/06/2018;*

*Căn cứ Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ về việc quy định chi tiết một số điều của Luật An ninh mạng;*

*Căn cứ Nghị định 47/2020/NĐ-CP ngày 09/04/2020 của Chính phủ về quản lý, kết nối chia sẻ dữ liệu số của cơ quan nhà nước;*

*Căn cứ Thông tư số 12/TT-BTTTT ngày 12/08/2022 của Bộ Thông tin và Truyền thông về việc quy định chi tiết và hướng dẫn 1 số điều của Nghị định số 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ về đảm bảo an toàn hệ thống thông tin theo cấp độ;*

*Theo đề nghị của Giám đốc Trung tâm Học liệu – Thư viện.*

## QUYẾT ĐỊNH

**Điều 1.** Ban hành kèm theo Quyết định này " Quy định Bảo đảm an toàn, an ninh mạng cho các Hệ thống thông tin của Trường Đại học Y khoa Vinh".

**Điều 2.** Quyết định có hiệu lực kể từ ngày ký.

**Điều 3.** Trưởng các đơn vị, viên chức, người lao động, người học của Trường Đại học Y khoa Vinh và các tổ chức, cá nhân có liên quan căn cứ Quyết định thi hành./.

***Nơi nhận:***
- Như điều 3;
- Lưu: VT.

**HIỆU TRƯỞNG**


**Nguyễn Văn Tuấn**

UBND TỈNH NGHỆ AN
**TRƯỜNG ĐHYK VINH**

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

# QUY ĐỊNH
## Bảo đảm an toàn, an ninh mạng cho các Hệ thống thông tin

*(Ban hành kèm theo Quyết định số 1285/QĐ-ĐHYKV ngày 22 tháng 8 năm 2023 của Hiệu Trưởng trường Đại học Y khoa Vinh)*

## Chương I

## QUY ĐỊNH CHUNG

### Điều 1. Phạm vi điều chỉnh

Quy định này được ban hành nhằm để quản lý, sử dụng mạng nội bộ, hộp thư điện tử và an toàn, an ninh thông tin trên không gian mạng của trường Đại học Y Khoa Vinh.

### Điều 2. Đối tượng áp dụng

Các phòng, đơn vị thuộc, trực thuộc trường Đại học Y Khoa Vinh (sau đây Đại học Y Khoa Vinh viết tắt là ĐHYKV); các cán bộ, viên chức, người lao động và người học, đơn vị thuộc, trực thuộc trường ĐHYKV trên không gian mạng tại nhà trường.

### Điều 3. Giải thích từ ngữ

Trong quy định này, các từ ngữ dưới đây được hiểu như sau:

1. Mạng nội bộ Trường đại học Y Khoa Vinh bao gồm: Hệ thống máy chủ, hệ thống máy Trạm, đường truyền (có dây, không dây), các thiết bị kết nối và được viết tắt là mạng LAN.

2. Trang thông tin điện tử của trường có địa chỉ là: http://www.vmu.edu.vn.

3. Hộp thư điện tử (email) của trường Đại học Y Khoa Vinh được cung cấp bởi dịch vụ Gmail của Google với tên miền là @vmu.edu.vn

4. Các đơn vị thuộc Trường bao gồm: khoa, phòng, trung tâm. Đơn vị trực thuộc: Bệnh viện trường. Các cá nhân được giao nhiệm vụ quản lý, các cán bộ, giảng viên, sinh viên của trường gọi chung là người dùng.

5. 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.

6. An ninh thông tin mạng 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.

7. Bảo đảm an toàn thông tin mức vật lý là việc bảo vệ hệ thống hạ tầng kỹ thuật, phần mềm, ứng dụng và cơ sở dữ liệu khỏi các mối nguy hiểm vật lý(như: cháy, nổ; nhiệt độ, độ ẩm ngoài mức cho phép; thiên tai; mất điện; tác động cơ học) có thể gây ảnh hưởng đến hoạt động của hệ thống;

8. Không gian mạng là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng internet, hệ thống máy tính, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian;

9. Hạ tầng kỹ thuật là tập hợp các thiết bị tính toán, lưu trữ, máy chủ, thiết bị ngoại vi, thiết bị kết nối mạng, thiết bị phụ trợ, đường truyền, mạng nội bộ, mạng diện rộng;

10. Hệ thống thông tin: Là 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 như: Hệ thống mạng nội bộ, hệ thống văn phòng điện tử, hệ thống thư điện tử, trang thông tin điện tử, …;

11. 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.

**Điều 4. Qui định chung**

1. Tuân thủ quy định về pháp luật khi sử dụng.

2. Nghiêm cấm sử dụng mạng máy tính của Nhà trường để truyên truyền, kích động, chống phá Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam.

3. Nghiêm cấm dưới mọi hình thức đối với việc phát tán các thông tin chưa được công bố của Nhà trường khi chưa có sự đồng ý của Hiệu trưởng nhà trường.

## Chương II

## HỘP THƯ ĐIỆN TỬ (EMAIL)

**Điều 5. Mục đích sử dụng**

1. Hộp thư điện tử nhằm mục đích hỗ trợ cho việc học tập, nghiên cứu trao đổi thông tin giữa nhà trường với sinh viên, giữa giảng viên với người học và liên lạc công việc bên ngoài. Ngoài ra thư điện tử cũng được dùng như một tài

khoản xác thực trong việc sử dụng các tiện ích Công nghệ thông tin đã và sẽ triển khai trên mạng nội bộ của nhà trường.

2. Hộp thư điện tử của nhà trường có dạng <tên người dùng>@vmu.edu.vn

3. Hộp thư điện tử của nhà trường sử dụng công nghệ, các tiện ích các bảo mật được cung cấp bởi Google.

**Điều 6. Qui định về trách nhiệm và qui trình cung cấp, thay đổi, xóa bỏ tài khoản hộp thư điện tử**

1. Cung cấp tài khoản Email

2. Mỗi cán bộ, giảng viên của trường được cung cấp 1 tài khoản email với tên miền @vmu.edu.vn

3. Thay đổi tài khoản email

4. Thông tin cá nhân: Khi có thay đổi về thông tin cá nhân của mình (tên, mật khẩu đăng nhập, ...) người dùng phải gửi thông tin theo mẫu đến phòng QLKH&HTQT để chịu trách nhiệm về tính xác thực này.

5. Xóa bỏ tài khoản Email ra khỏi hệ thống thư điện tử của trường: Đối với cán bộ giảng viên của trường Email cá nhân được duy trì trong suốt thời gian còn làm việc tại trường. Định kỳ 06 tháng phòng tổ chức cán bộ có trách nhiệm cung cấp danh sách biến động nhân sự của trường cho cán bộ Bộ phận Công nghệ thông tin để cập nhật lại Email của trường.

**Điều 7. Quy định về sử dụng hộp thư điện tử**

1. Việc trao đổi thông tin trong công việc thuộc phạm vi nhà Trường phải thông qua địa chỉ Email với tên miền là @vmu.edu.vn.

2. Nội dung thư điện tử phải minh bạch, rõ ràng, nếu gõ tiếng Việt phải sử dụng font Unicode.

3. Tài khoản hộp thư điện tử của người dùng ngoài việc là công cụ giao tiếp, trao đổi công việc còn được dùng là định danh trong việc xác thực sử dụng các tiện ích CNTT được triển khai trong nhà Trường. Do đó người dùng phải có trách nhiệm bảo vệ hộp thư điện tử của mình và tuân thủ các quy định sử dụng.

4. Mật khẩu tài khoản email phải được giữ cẩn thận nhằm tránh trường hợp người khác sử dụng mật khẩu để gửi thư có nội dung không lành mạnh. Nên thường xuyên thay đổi mật khẩu.

5. Người dùng phải thường xuyên kiểm tra hộp thư điện tử cá nhân hàng

ngày để nhận và trao đổi thông tin với nhà trường, bên ngoài nhằm phục vụ công việc.

6. Người dùng phải chịu trách nhiệm trước pháp luật và Nhà nước về nội dung trong hộp thư trong thời gian tài khoản còn hiệu lực. Nghiêm cấm sử dụng hộp thư điện tử cho các mục đích sau:

- Phát tán nội dung mang thông tin không lành mạnh, có nội dung đả kích, xuyên tạc sai sự thật hoặc quấy rối người khác.

- Phát tán vi rút hoặc phần mềm phá hoại.

- Phát tán các thông tin quảng cáo.

- Lưu trữ các nội dung trái phép với quy định của pháp luật.

- Tấn công các máy chủ của nhà trường và các nơi khác.

- Giả mạo thư điện tử dưới danh nghĩa một người khác.

## Chương III

## QUẢN LÝ, SỬ DỤNG MẠNG NỘI BỘ, MẠNG INTERNET, DATA CENTER

### Điều 8. Quản lý, vận hành mạng nội bộ (LAN), kết nối Internet

1. Trung tâm Học liệu - Thư viện trực tiếp quản lý, vận hành mạng nội bộ, kết nối Internet của Trường, đảm bảo mạng hoạt động thông suốt 24h/24h. Trung tâm Học liệu - Thư viện là đầu mối tập trung kết nối mạng, hướng dẫn sử dụng mạng, hướng dẫn khai thác và quản lý mạng cho tất cả các đơn vị trong Trường.

2. Thường xuyên kiểm tra, theo dõi, đánh giá hoạt động của mạng nội bộ, kết nối Internet, thiết bị mạng, hệ thống Data Center và các thiết bị tin học khác theo đúng tiêu chuẩn kỹ thuật; thực hiện công tác bảo trì, bảo dưỡng định kỳ, đột xuất, giảm thiểu tối đa các sự cố kỹ thuật liên quan.

3. Các cá nhân, đơn vị thuộc Trường khi tham gia vào mạng Lan không được tự ý thay đổi các tham số mạng, đề nghị liên hệ với Trung tâm Học liệu - Thư viện để được hỗ trợ.

### Điều 9. Phần mềm trên hệ thống mạng nội bộ trường

1. Phần mềm được phép hoạt động trên hệ thống mạng nội bộ nhà trường bao gồm hệ điều hành Windows, IOS, ứng dụng Office từ phiên bản 2010 trở lên, bộ gõ Vietkey/Unikey, ứng dụng Anti Virus, các trình duyệt Web (Chrome, Firefox) và các phần mềm hỗ trợ hoc tập, nghiên cứu khác.

2. Trung tâm Học liệu - Thư viện có trách nhiệm cài đặt các phần mềm nói trên lên các máy chủ, máy trạm hoạt động trong hệ thống mạng nội bộ nhà trường và hướng dẫn sử dụng cho các cá nhân, đơn vị theo yêu cầu của công việc.

3. Ngoài các phần mềm như đã nêu ở trên, nghiêm cấm cá nhân, đơn vị tự ý cài đặt các phần mềm khác. Trong trường hợp có nhu cầu cài đặt các phần mềm để phục vụ hoạt động quản lý hoặc các hoạt động chuyên môn khác thì phải thông báo cho Trung tâm Học liệu - Thư viện để được hỗ trợ lựa chọn phương án cài đặt tối ưu.

**Điều 10. Nghiêm cấm người dùng sử dụng mạng nội bộ, kết nối internet trong trường để:**

1. Chơi các trò chơi trực tuyến (game online) hoặc các trò chơi khác trên Internet trong giờ làm việc; Tùy ý kết nối, khai thác, lưu trữ các thông tin, các trò chơi, các chương trình giải trí có nội dung xấu, không lành mạnh; Tự động truy cập vào các mạng không dây lân cận không rõ nguồn gốc; chia sẻ tài nguyên cho bất cứ đối tượng nào khi chưa được phép của Lãnh đạo nhà trường.

2. Tạo đường dẫn trái phép đối với tên miền hợp pháp của tổ chức, cá nhân; Tạo, cài đặt, phát tán phần mềm độc hại, virus máy tính; Xâm nhập trái phép, chiếm quyền điều khiển hệ thống thông tin, tạo lập công cụ tấn công trên Internet.

3. Tự ý mạng dữ liệu, cài đặt lên máy tính hoặc chạy chương trình các phần mềm không rõ nguồn gốc, không có bản quyền;

4. Truy cập hoặc tải các trang Website, các chương trình, các thông tin quảng cáo không rõ nguồn gốc…

5. Mở bất cứ thư điện tử, tệp đính kèm, đường link, thư rác, thư quảng cáo không rõ nguồn gốc và không xác định được người gửi khi sử dụng hệ thống thư điện tử của nhà trường.

## Chương IV
## AN TOÀN THÔNG TIN VÀ AN NINH MẠNG TRONG MẠNG NỘI BỘ

**Điều 11. An toàn thông tin và An ninh mạng**

1. Để đảm bảo an toàn và bảo mật thông tin dữ liệu trên mạng nội bộ, trên internet, Trung tâm Học liệu - Thư viện và người dung phải có trách nhiệm thực hiện nghiêm túc các quy định, hướng dẫn liên quan đến an toàn thông tin và an ninh mạng.

2. Khi phát hiện thấy yếu tố không an toàn đối với mạng nội bộ xuất phát từ bất cứ nơi đâu trên mạng hoặc máy trạm nào, người dùng thông báo ngay cho Trung tâm Học liệu - Thư viện để có biện pháp xử lý kịp thời.

3. Trung tâm Học liệu - Thư viện sẽ hủy tài khoản cá nhân và ngắt kết nối ngay lập tức đối với các cá nhân, đơn vị có hành vi cố ý tấn công hoặc gây trở ngại và mất an toàn thông tin cũng như an ninh cho mạng nội bộ Trường.

4. Các máy tính tham gia mạng nội bộ Trường phải được cài đặt, cập nhật và quét virus ba tháng một lần. Trung tâm Học liệu - Thư viện chịu trách nhiệm cung cấp chương trình quét vius, bản cập nhật và hướng dẫn sử dụng.

5. Khi người dùng gặp trục trặc về kết nối mạng, máy tính, virus máy tính,… và cần sự hỗ trợ, đề nghị liên hệ với Trung tâm Học liệu - Thư viện. Trung tâm Học liệu - Thư viện có trách nhiệm hướng dẫn trực tuyến hoặc cử nhân viên đến hỗ trợ trong thời gian nhanh nhất.

**Điều 12. Trách nhiệm – Quyền hạn của Trung Tâm Học liệu – Thư viện trong việc đảm bảo an toàn thông tin và an ninh mạng**

1. Trung tâm Học liệu - Thư viện là nơi duy nhất trong Trường có quyền cài đặt phần mềm, thiết lập các chính sách bao gồm phân quyền điều khiển từ xa trên máy trạm thuộc mạng nội bộ Trường nhằm đảm bảo an toàn cho hệ thống mạng máy tính.

2. Trung tâm Học liệu - Thư viện đề xuất và phối hợp với nhà cung cấp dịch vụ bảo mật triển khai thiết lập hệ thống tường lửa (bằng phần cứng hoặc proxy server) để ngăn chặn việc xem các video clip, phim, nhạc trực tuyến, trò chơi trực tuyến hoặc các ứng dụng không phục vụ mục đích công việc tại trường nhằm đảm bảo tốc độ truy cập mạng cũng như an toàn an ninh thông tin trên mạng.

3. Khi phát hiện máy tính trong mạng bị nhiễm và phát tán virus, Trung tâm Học liệu - Thư viện thông báo cho người dùng và ngắt kết nối để xử lý.

4. Trung tâm Học liệu - Thư viện có quyền thiết lập các quy định riêng (sau khi được Hiệu trưởng phê duyệt) để đảm bảo an toàn an ninh cho hệ thống mạng và phù hợp với thực tế phát triển của công nghệ thông tin hiện tại và thông báo hướng dẫn đến người dùng.

## Chương V

## TỔ CHỨC THỰC HIỆN

**Điều 13. Trách nhiệm thi hành**

1. Trưởng các đơn vị có trách nhiệm phổ biến, quán triệt đến toàn bộ

cán bộ, viên chức và người lao động trong đơn vị thực hiện quy định.

2. Trung tâm Học liệu - Thư viện chủ trì và phối hợp với các phòng ban hướng dẫn việc thực hiện quản lý, sử dụng mạng nội bộ, kết nối internet và xử lý sự cố máy tính tai trường.

3. Các đơn vị cùng toàn thể viên chức, người lao động và người học có trách nhiệm thực hiện nghiêm túc quy định này.

**Điều 14. Xử lý vi phạm**

Viên chức, người lao động và người học có hành vi phạm thì bị xử lý theo quy định của pháp luật và nội quy của nhà trường.

**Điều 15. Sửa đổi, bổ sung**

Các đơn vị thuộc, trực thuộc có trách nhiệm theo dõi, kiểm tra, đôn đốc việc thực hiện quy định này. Trung tâm Học liệu -` Thư viện tổng hợp các ý kiến góp ý, nghiên cứu đề xuất kịp thời việc bổ sung, sửa đổi quy định, phù hợp với yêu cầu công tác của trường.

**Điều 16. Hiệu lực và thi hành**

Quy định này có hiệu lực thi hành kể từ ngày ký./.