

Huế, ngày 15 tháng 9 năm 2021

QUY ĐỊNH

Bảo mật thông tin, an ninh mạng

I. Phạm vi và đối tượng áp dụng

1. Quy định về công tác đảm bảo bảo mật thông tin trong hoạt động công nghệ thông tin (CNTT) của các khoa, phòng ban trực thuộc Đại học Phú Xuân

2. Quy định này áp dụng đối với các khoa, phòng ban và các giảng viên, cán bộ thuộc Trường Đại học Phú Xuân.

II. Phạm vi và tài nguyên đảm bảo bảo mật thông tin

1. Hệ thống mạng của Trường Đại học Phú Xuân gồm:

- Hệ thống đường truyền dữ liệu, đường kết nối Internet;
- Hệ thống mạng có dây, không dây;
- Các trang thiết bị CNTT được kết nối mạng trong đơn vị.

2. Hệ thống tài nguyên mạng và ứng dụng CNTT bao gồm:

- Hệ thống thư điện tử;
- Hệ thống thông tin quản lý và cơ sở dữ liệu đào tạo, tuyển sinh, kế toán, nhân sự;
- Cổng thông tin điện tử và hệ thống website;

III. Nguyên tắc chung triển khai công tác an toàn thông tin

1. An toàn thông tin phải được đảm bảo trong quá trình thiết kế, xây dựng, vận hành hệ thống CNTT.

2. Khi thuê dịch vụ CNTT hoặc sử dụng dịch vụ thông tin do bên thứ ba cung cấp, nhà trường phải làm chủ thông tin, dữ liệu trên hệ thống dịch vụ đó. Tuyệt đối không để nhà cung cấp dịch vụ truy cập, sử dụng thông tin, dữ liệu trong phạm vi nhà trường quản lý.

IV. Các hành vi bị nghiêm cấm

1. Ngăn chặn trái phép việc truyền tải thông tin trên mạng; can thiệp trái phép, gây nguy hại, xóa, thay đổi, sửa chữa, làm sai lệch thông tin trên mạng.



2. Ngăn chặn trái phép, gây ảnh hưởng tới sự hoạt động bình thường của hệ thống thông tin hoặc ngăn chặn trái phép, gây ảnh hưởng tới khả năng truy cập hợp pháp của người sử dụng tới hệ thống thông tin.

3. Lợi dụng sơ hở, điểm yếu của hệ thống thông tin để cố ý vượt qua biện pháp kiểm soát truy cập, tấn công, chiếm quyền điều khiển trái phép đối với hệ thống thông tin.

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

5. Truy cập bất hợp pháp thông tin của cá nhân hoặc tổ chức.

6. Làm thay đổi hệ thống mạng: tự ý lắp đặt thêm bộ chuyển mạch (switch), lắp đặt thêm mạng không dây, cấu hình địa chỉ IP,...

7. Cấm lưu trữ, đưa lên mạng hoặc trao đổi các thông tin sau:

a) Thông tin chưa được cấp có thẩm quyền công bố.

b) Thông tin thuộc danh mục thông tin mật do pháp luật hiện hành quy định.

c) Thông tin và các dịch vụ thông tin trái với quy định của pháp luật hiện hành như:

- Gây ảnh hưởng đến an ninh quốc gia;

- Xuyên tạc, tuyên truyền chống đối chính sách và pháp luật của Nhà nước;

- Có nội dung kích động bạo lực, tuyên truyền chiến tranh xâm lược, gây hận thù giữa các dân tộc và nhân dân các nước, truyền bá tư tưởng phản động;

- Có ảnh hưởng đến văn hoá xã hội và thuần phong mỹ tục;

- Giả mạo nguồn gốc của thông tin;

- Có ảnh hưởng xấu đến đời tư người khác: quấy rối cá nhân, xúc phạm danh dự, vu khống, xúc phạm đến nhân phẩm người khác.

V. Yêu cầu về công tác bảo đảm an toàn thông tin

1. Hệ thống mạng nội bộ của nhà trường thường xuyên được quản lý, giám sát, kiểm soát nhằm phát hiện và ngăn chặn các truy cập trái phép của người sử dụng và tin tặc; cần được triển khai cơ chế phòng chống vi rút tin học, thư rác cho hệ thống thư điện tử, máy tính.

2. Có biện pháp bảo vệ, phòng và chống các nguy cơ mất cắp thông tin, cháy nổ, ngập lụt nước và các thảm hoạ do thiên nhiên hoặc con người gây ra và có các phương án khắc phục sau thảm hoạ.

3. Xây dựng hệ thống dự phòng cho các hệ thống CNTT cốt lõi như: máy chủ web, cơ sở dữ liệu, thư điện tử. Phải có quy trình phục hồi, sao lưu dữ liệu định kỳ cho hệ thống các phần mềm và cơ sở dữ liệu.

4. Quản lý chặt chẽ hệ thống tài khoản người sử dụng của các hệ thống thông tin, thư điện tử, và các tài nguyên mạng khác gồm các công việc: tạo mới, kích hoạt, sửa đổi, vô hiệu hoá, xoá bỏ,... Phải có biện pháp khóa hoặc hủy tài khoản, quyền truy nhập, thu hồi các thiết bị liên quan tới hệ thống thông tin cho phù hợp đối với cán bộ, công chức, viên chức đã nghỉ việc hoặc chuyển công tác.

VI. Một số biện pháp quản lý vận hành đảm bảo an toàn thông tin

1. Đối với cán bộ phụ trách công nghệ thông tin:

a) Tham mưu cho lãnh đạo triển khai thực hiện các biện pháp để đảm bảo an toàn, an ninh hệ thống thông tin của cơ quan, đơn vị. Thường xuyên nghiên cứu, cập nhật các kiến thức về bảo mật thông tin, có biện pháp phòng tránh các nguy cơ tiềm ẩn có thể gây mất thông tin khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ.

b) Thường xuyên cập nhật cấu hình chuẩn cho các thành phần của hệ thống thông tin, thiết lập cấu hình chặt chẽ nhất nhưng vẫn đảm bảo duy trì hoạt động thường xuyên của hệ thống thông tin.

c) Khi thiết lập cấu hình hệ thống thông tin cần xác định các chức năng, cổng giao tiếp mạng, giao thức và dịch vụ không cần thiết để cấm hoặc hạn chế sử dụng.

đ) Kiểm soát chặt chẽ việc cài đặt phần mềm vào các máy tính thuộc các phòng ban.

3. Đối với cán bộ, công chức, viên chức:

a) Thường xuyên cập nhật những chính sách, thủ tục an toàn thông tin của nhà trường và thực hiện đúng hướng dẫn về công nghệ thông tin của cán bộ phụ trách.

b) Thực hiện quét vi rút trước khi mở các tập tin đính kèm theo thư điện tử, không mở các thư điện tử khi chưa rõ người gửi hoặc tập tin đính kèm có nguồn gốc không rõ ràng để tránh vi rút, phần mềm gián điệp lây nhiễm máy tính.

c) Phải đặt mật khẩu cho máy tính (mật khẩu đăng nhập, mật khẩu bảo vệ màn hình). Sử dụng các thiết bị lưu trữ thông tin (USB, ổ cứng gắn ngoài, thẻ nhớ,...) đảm bảo an toàn, đúng cách để phòng ngừa vi rút, phần mềm gián điệp xâm nhập

máy tính phá hoại, đánh cắp thông tin. Định kỳ thường xuyên quét vi rút, phần mềm gián điệp trên máy tính.

VII. Một số biện pháp quản lý kỹ thuật đảm bảo an toàn thông tin

1. Quản lý hệ thống mạng:

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:

Khi thiết lập mạng không dây để kết nối với mạng cục bộ thông qua các điểm truy nhập, cần thiết lập các tham số như: Tên, mật khẩu, mã hóa dữ liệu và thông báo các thông tin liên quan đến điểm truy nhập để nhà trường sử dụng, thường xuyên thay đổi mật khẩu nhằm tăng cường công tác bảo mật.

3. Quản lý đăng nhập hệ thống:

- Tăng cường áp dụng biện pháp bảo mật hai lớp (2-step verification) đối với những ứng dụng quan trọng về bảo mật thông tin.

- Có biện pháp khoá, chặn quyền truy nhập tới hệ thống đối với những tài khoản có dấu hiệu hoặc bị rò rỉ thông tin truy cập.

- Yêu cầu người dùng đặt mật khẩu với độ an toàn cao (có chữ thường, có chữ in hoa, có số và ký tự đặc biệt như @, #, !,...) và thường xuyên thay đổi mật khẩu 1 lần/tháng.

4. Chống mã độc, vi rút:

Lựa chọn, triển khai các phần mềm chống vi rút, thư rác có hiệu quả trên các máy chủ, máy trạm, các thiết bị, phương tiện kỹ thuật trong mạng, các hệ thống thông tin quan trọng như: Cổng/Trang thông tin điện tử, thư điện tử, một cửa điện tử,..; đồng thời, thường xuyên cập nhật phiên bản mới, bản vá lỗi của các phần mềm chống vi rút, nhằm kịp thời phát hiện, loại trừ mã độc máy tính (vi rút, trojan, worms,..).

5. Các biện pháp kỹ thuật bảo đảm an toàn cho website:

- Xác định cấu trúc thiết kế website: Quản lý toàn bộ các phiên bản của mã nguồn, phối hợp với đơn vị thực hiện dịch vụ thuê máy chủ (hosting) tổ chức mô hình trang web hợp lý tránh khả năng tấn công leo thang đặc quyền. Yêu cầu đơn vị

cung cấp dịch vụ hosting phải cài đặt các hệ thống phòng vệ như tường lửa (firewall), thiết bị phát hiện/phòng chống xâm nhập (IDS/IPS) ở mức ứng dụng web (WAF - Web Application Firewall).

- Vận hành ứng dụng website an toàn: Các website khi đưa vào sử dụng hoặc khi bổ sung thêm các chức năng, dịch vụ công mới cần đánh giá kiểm định nhằm tránh được các lỗi bảo mật thường xảy ra trên ứng dụng web.

- Thiết lập và cấu hình cơ sở dữ liệu an toàn:

- Gỡ bỏ các cơ sở dữ liệu không sử dụng;

- Phối hợp với các nhà cung cấp dịch vụ hosting xây dựng phương án phục hồi website, trong đó chú ý ít nhất mỗi tháng thực hiện việc sao lưu toàn bộ nội dung trang web 01 lần bao gồm mã nguồn, cơ sở dữ liệu, dữ liệu phi cấu trúc để bảo đảm khi có sự cố có thể khắc phục trong thời gian ngắn nhất.

6. Thiết lập cơ chế sao lưu và phục hồi hệ thống:

Hệ thống thông tin phải có cơ chế sao lưu thông tin ở mức người dùng và mức hệ thống, được lưu trữ tại nơi an toàn; đồng thời, thường xuyên kiểm tra để đảm bảo tính sẵn sàng phục hồi và toàn vẹn thông tin. Có giải pháp sao lưu dự phòng dữ liệu ra chỗ khác nhằm tránh tình trạng hỏa hoạn, thiên tai, lũ lụt.

7. Xử lý khẩn cấp:

Khi phát hiện hệ thống máy chủ bị tấn công, thông qua các dấu hiệu như luồng tin tăng lên bất ngờ, nội dung trang chủ bị thay đổi, hệ thống hoạt động rất chậm khác thường,... cần thực hiện các bước cơ bản sau:

a) Bước 1: Ngắt kết nối máy chủ ra khỏi mạng.

b) Bước 2: Sao chép logfile và toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ (phục vụ cho công tác phân tích).

c) Bước 3: Khôi phục hệ thống bằng cách chuyển dữ liệu dự phòng (backup) mới nhất để hệ thống hoạt động.

d) Bước 4: Thông báo cho cơ quan chức năng để được hướng dẫn, hỗ trợ.

VIII. Trách nhiệm của cán bộ, công chức, viên chức trong nhà trường.

1. Trách nhiệm của cán bộ phụ trách công nghệ thông tin:



a) Chịu trách nhiệm triển khai các biện pháp quản lý vận hành, quản lý kỹ thuật, tham mưu xây dựng quy định về đảm bảo an toàn, an ninh cho hệ thống thông tin của cơ quan, đơn vị theo Quy chế này và phân công của Thủ trưởng đơn vị.

b) Phối hợp với các cá nhân, đơn vị có liên quan trong việc kiểm tra, phát hiện và khắc phục các sự cố mất an toàn thông tin .

2. Trách nhiệm của cán bộ, công chức, viên chức:

a) Chấp hành nghiêm túc các quy định về an toàn thông tin của quy định này và các quy định khác của pháp luật; nâng cao ý thức cảnh giác và trách nhiệm đảm bảo an ninh thông tin tại cơ quan, đơn vị.

b) Khi phát hiện sự cố phải báo ngay với cấp trên và bộ phận phụ trách công nghệ thông tin để kịp thời ngăn chặn, xử lý.



TS. Hồ Thị Hạnh Tiên