BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC VÕ TRƯỜNG TOẢN
Số: 512/QĐ-ĐHVTT-TCHC

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

Hậu Giang, ngày 12 tháng 11 năm 2019

QUYẾT ĐỊNH
V/v Ban hành Quy định về đảm bảo an toàn thông tin, bảo mật cho hệ thống thông tin đảm bảo chất lượng bên trong tại Trường Đại học Võ Trường Toản

HIỆU TRƯỞNG TRƯỜNG ĐẠI HỌC VÕ TRƯỜNG TOẢN

Căn cứ Quyết định số 196/QĐ-TTg ngày 18 tháng 02 năm 2008 của Thủ tướng Chính phủ về việc thành lập Trường Đại học Võ Trường Toản;

Căn cứ vào Quy chế Tổ chức và hoạt động của Trường Đại học Võ Trường Toản;

Căn cứ Luật An ninh mạng số 24/2018/QH14 ngày 12 tháng 6 năm 2018;

Xét đề nghị của Trưởng Phòng Tổ chức Hành chính,

QUYẾT ĐỊNH:

Điều 1. Ban hành "Quy định về đảm bảo an toàn thông tin, bảo mật cho hệ thống thông tin đảm bảo chất lượng bên trong tại Trường Đại học Võ Trường Toản" kèm theo Quyết định này.

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

Điều 3. Trưởng Phòng Tổ chức Hành chính, các đơn vị trực thuộc và và các cá nhân, tổ chức có liên quan chịu trách nhiệm thi hành quyết định này./.

Nơi nhận:
- Như Điều 3;
- Lưu: VT, TC.

HIỆU TRƯỞNG

(đã ký)

Dương Đăng Khoa

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC VÕ TRƯỜNG TOẢN

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

QUY ĐỊNH
Đảm bảo an toàn thông tin, bảo mật cho hệ thống thông tin đảm bảo chất lượng bên trong tại Trường Đại học Võ Trường Toản

(Ban hành kèm theo Quyết định số 512/QĐ-ĐHVTT-TCHC ngày 12/11/2019 của Hiệu trưởng Trường Đại học Võ Trường Toản)

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. Quy định này ban hành Quyết định này quy định các yêu cầu đảm bảo thông suốt, an toàn, bảo mật thông tin cho việc ứng dụng công nghệ thông tin trong việc quản lý, sử dụng, lưu trữ, truyền đưa các thông tin đảm bảo chất lượng (ĐBCL) bên trong.

2. Quy định này áp dụng đối với các đơn vị tại Trường Đại học Võ Trường Toản (VTTU) triển khai ứng dụng công nghệ thông tin trong quản lý, sử dụng, lưu trữ, truyền đưa thông tin ĐBCL bên trong.

Điều 2. Quy định về máy chủ

1. Bảo đảm có hạ tầng máy chủ và các thiết bị đi kèm phục vụ hệ thống thông tin đủ công suất, đảm bảo tốc độ xử lý truy xuất thông tin đáp ứng yêu cầu của đơn vị.

2. Máy chủ phải được đặt ở phòng riêng, được bảo vệ an toàn về mặt vật lý (phải được khóa và được giám sát chặt chẽ). Đảm bảo trang bị nguồn điện, nhiệt độ phục vụ cho hoạt động liên tục của máy chủ. Có các phương án phòng chống cháy, nổ cho phòng máy chủ. Phân công trách nhiệm của những cá nhân được phép vào phòng máy chủ.

3. Việc truy cập máy chủ đều phải thông qua kiểm soát bằng mật khẩu hoặc các biện pháp kiểm soát phù hợp khác.

4. Có biện pháp phát hiện, phòng chống xâm nhập, phát tán mã độc hại và virus máy tính cho máy chủ.

Điều 3. Quy định về máy trạm

1. Máy trạm (bao gồm máy tính để bàn và máy tính xách tay) phải được bảo vệ bằng mật khẩu.

3. Phải có phương án phát hiện, phòng chống xâm nhập, phát tán mã độc hại và virus cho máy trạm.

4. Phải có phương án bảo vệ dữ liệu máy trạm nếu kết nối với mạng Internet.

5. Đối với các máy trạm trực tiếp làm việc với người học và các bên liên quan cần đảm bảo thông tin ĐBCL bên trong trên màn hình máy tính trong lúc làm việc không được xem bởi các cá nhân không được phép. Đặt chế độ khóa màn hình khi không làm việc trên máy tính.

Điều 4. Quy định về mạng nội bộ và Internet

1. Có biện pháp phát hiện và phòng chống xâm nhập, phòng chống phát tán mã độc hại trên mạng nội bộ và Internet.

2. Có biện pháp phòng chống tấn công từ chối dịch vụ từ bên trong mạng nội bộ và bên ngoài Internet.

3. Yêu cầu có các biện pháp xác thực đảm bảo an toàn đối với các kết nối không dây.

4. Đảm bảo kiểm soát được các truy cập hệ thống thông tin và đảm bảo truy cập hiệu quả đối với các dữ liệu cần truy cập nhanh chóng.

5. Thiết lập các phương án dự phòng cho các vị trí có mức độ ảnh hưởng cao tới hoạt động của hệ thống mạng hoặc có khả năng làm tê liệt hệ thống mạng của đơn vị khi xảy ra sự cố.

6. Thường xuyên cập nhật các bản vá lỗi hệ thống, cập nhật cấu hình cho các thiết bị mạng và các thiết bị bảo mật.

Điều 5. Cơ sở dữ liệu

1. Chỉ được sử dụng hệ quản trị cơ sở dữ liệu có bản quyền, nguồn gốc, xuất xứ rõ ràng, hoặc các hệ quản trị cơ sở dữ liệu mã nguồn mở nhưng được sử dụng rộng rãi.

2. Hệ quản trị cơ sở dữ liệu sử dụng cho hệ thống thông tin của đơn vị cần đáp ứng được yêu cầu hoạt động ổn định; xử lý, lưu trữ được khối lượng dữ liệu của đơn vị theo yêu cầu nghiệp vụ; có cơ chế bảo vệ và phân quyền truy cập đối với các tài nguyên cơ sở dữ liệu.

3. Thường xuyên rà soát, cập nhật các bản vá, các bản sửa lỗi hệ quản trị cơ sở dữ liệu.

4. Xây dựng phương án sao lưu, dự phòng đối với cơ sở dữ liệu, đảm bảo khôi phục dữ liệu nhanh chóng khi có sự cố xảy ra.

5. Thực hiện phân quyền và có quy định chặt chẽ với từng cá nhân truy cập đến cơ sở dữ liệu, khuyến khích việc ghi nhật ký đối với các truy cập và các thao tác cơ sở dữ liệu nhưng phải không ảnh hưởng đến tốc độ xử lý dữ liệu của cơ sở dữ liệu.

6. Yêu cầu có các phương án ngăn chặn các hình thức tấn công và truy cập cơ sở dữ liệu trái phép.

7. Mọi thông tin của các bên liên quan trên hệ thống công nghệ thông tin được bảo mật theo yêu cầu của Nhà trường.

8. Hệ thống công nghệ thông tin của Nhà trường được bảo vệ bằng mật mã bảo vệ. Liên tục có sự theo dõi thường xuyên của người quản trị nhằm ngăn chặn sự truy cập trái phép hoặc khả nghi. Mật khẩu của các bên liên quan được mã hóa một chiều, ngay cả người quản trị server cũng không thể biết được mật khẩu của các bên liên quan.

9. Khi gặp sự cố bảo mật, các bên liên quan cần phải liên hệ với Nhà trường để phối hợp xử lý.

Điều 6. Sao lưu, phục hồi

1. Đối với dữ liệu trên máy tính cá nhân:

- Đối với các dữ liệu quan trọng, sao lưu cần được thực hiện khi dữ liệu có sự thay đổi. Đảm bảo các dữ liệu quan trọng được phục hồi nguyên vẹn khi cần thiết.

- Đảm bảo dữ liệu cần thiết trên máy tính đều được sao lưu khi có các thay đổi hoặc nâng cấp bất kỳ đối với hệ điều hành.

- Dữ liệu sao lưu phải được lưu ở vị trí an toàn, cách xa dữ liệu gốc và những người không được cho phép. Đối với những dữ liệu quan trọng, khuyến khích dữ liệu sao lưu đặt cách xa vị trí địa lý của đơn vị.

2. Đối với cơ sở dữ liệu trên máy chủ:

- Các dữ liệu sao lưu và các bản sao lưu hoàn chỉnh của cơ sở dữ liệu và tài liệu quy trình phục hồi phải được lưu trữ ở các địa điểm cách xa vị trí cài đặt để đảm bảo tránh khỏi các sự cố nghiêm trọng nếu có.

- Phương tiện sao lưu phải được kiểm tra thường xuyên để sẵn sàng sử dụng trong trường hợp khẩn cấp.

- Cần xác định thời gian lưu trữ cho các thông tin quan trọng và các yêu cầu cho các bản sao lưu trữ vĩnh viễn.

- Quy trình phục hồi cơ sở dữ liệu phải được kiểm tra thường xuyên để đảm bảo hiệu quả và có thể hoàn thành trong thời gian cho phép.

Điều 7. Bảo mật tài khoản

1. Mọi thông tin tài khoản của các bên liên quan tương tác với hệ thống công nghệ thông tin của Nhà trường đều thông qua việc nhận gửi thư điện tử (email). Vì vậy, để đảm bảo thông tin cá nhân của mình, các cá nhân liên quan cần phải bảo mật thông tin email cá nhân.

2. Không ghi thông tin tài khoản ra bất kỳ đâu, cần tự ghi nhớ.

3. Nhà trường sẽ không yêu cầu các cá nhân liên quan cung cấp mật khẩu của tài khoản để đảm bảo chỉ mỗi cá nhân liên quan là người duy nhất biết mật khẩu đó. Khuyến cáo không lựa chọn các con số dễ đoán để làm mật khẩu như ngày sinh nhật, số điện thoại hoặc một phần tên mình. Nếu cá nhân phát hiện thông tin tài khoản hay mã bí mật tiết lộ cho bên thứ ba, bị mất cắp từ đó nảy sinh các thông tin trao đổi không do chính mình tiến hành, cần có trách nhiệm thông báo cho Nhà trường ngay lập tức.

4. Cả Nhà trường và các bên liên quan đều đóng vai trò quan trọng trong việc chống gian lận. Các cá nhân liên quan có trách nhiệm không tiết lộ thông tin tài khoản của mình cho người khác theo cách cố tình hay vô ý.

Điều 8. Trao đổi thông tin ĐBCL bên trong trên môi trường mạng

1. Sử dụng các phương pháp định danh phù hợp với quy định của Pháp luật và đơn vị.

2. Sử dụng các phương pháp mã hóa phù hợp đáp ứng yêu cầu bảo mật và khả năng xử lý của hệ thống thông tin để bảo mật thông tin ĐBCL bên trong.

3. Đảm bảo khôi phục được các thông tin đã mã hóa khi cần thiết.

Điều 9. Đảm bảo tính liên tục của hệ thống thông tin

1. Xây dựng, ban hành phương án đảm bảo tính liên tục của hệ thống thông tin.

2. Có phương án sao lưu, phục hồi dữ liệu.

3. Đảm bảo việc truy cập dữ liệu nhanh chóng, không gián đoạn.

4. Có phương án đảm bảo dự phòng hệ thống mạng.

5. Có phương án đảm bảo tính liên tục của hệ thống máy chủ. Khuyến khích sử dụng các công nghệ đảm bảo tính sẵn sàng cho hệ thống máy chủ.

Điều 10. Trách nhiệm thi hành

1. Quyết định này có hiệu lực kể từ ngày ký.

2. Trong quá trình thực hiện, Hiệu trưởng xem xét, quyết định việc tiếp thu và kiến nghị sửa đổi quy định cho phù hợp với thực tiễn trên cơ sở đề xuất của các cá nhân, tổ chức có liên quan./.