BỘ XÂY DỰNG
TRƯỜNG ĐHXD MIỀN TÂY

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

Số 457/QĐ-ĐHXDMT

Vĩnh Long, ngày 07 tháng 11 năm 2019

QUYẾT ĐỊNH

Ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các đơn vị thuộc Trường Đại học Xây dựng Miền Tây

HIỆU TRƯỞNG
TRƯỜNG ĐẠI HỌC XÂY DỰNG MIỀN TÂY

Căn cứ Quyết định số 1528/QĐ-TTg ngày 06/9/2011 của Thủ tướng Chính phủ về việc thành lập Trường Đại học Xây dựng Miền Tây;

Căn cứ Quyết định số 343/QĐ-ĐHXDMT ngày 17/10/2018 của Hiệu trưởng về việc ban hành quy chế tổ chức và hoạt động Trường Đại học Xây dựng Miền Tây;

Căn cứ Luật An ninh mạng số 24/2018/QH14 ngày 01/01/2019;

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ quy định về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

Căn cứ Nghị định số 27/2018/NĐ-CP ngày 01/3/2018 của Chính phủ về việc sửa đổi, bổ sung một số điều của Nghị định số 72/2013/NĐ-CP ngày 15/7/2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng;

Theo đề nghị của Phòng Quản lý Đào tạo.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các đơn vị thuộc Trường Đại học Xây dựng Miền Tây

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

Điều 3. Phòng Quản lý Đào tạo, Trưởng các đơn vị và toàn thể viên chức, người lao động và sinh viên trong Nhà trường chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- BGH;
- Như điều 3;
- Lưu: VT, QLĐT.

HIỆU TRƯỞNG

TRƯỜNG ĐẠI HỌC XÂY DỰNG MIỀN TÂY

Nguyễn Văn Xuân

BỘ XÂY DỰNG
TRƯỜNG ĐHXD MIỀN TÂY

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

QUY ĐỊNH
Đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các đơn vị thuộc Trường Đại học Xây dựng Miền Tây

(Ban hành kèm theo Quyết định số 457/QĐ-ĐHXDMT ngày 07 / 11/2019 của Hiệu trưởng Trường Đại học Xây dựng Miền Tây)

Chương I
QUI ĐỊNH CHUNG

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

1. Quy định này quy định về công tác đảm bảo an toàn thông tin điện tử (ATTT) trong hoạt động ứng dụng công nghệ thông tin (CNTT) của các đơn vị thuộc Trường Đại học Xây dựng Miền Tây.

2. Quy định này áp dụng cho các đơn vị, cá nhân thuộc Trường bao gồm các Phòng, Khoa, Trung tâm, Ban, Bộ môn, các tổ chức Đảng, đoàn thể, các cán bộ, giảng viên, sinh viên (sau đây gọi chung là các đơn vị, cá nhân).

Điều 2. Giải thích từ ngữ

1. *An toàn thông tin* là sự bảo vệ thông tin và các hệ thống thông tin 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.

2. *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.

3. *Xâm phạm ATTT* là hành vi truy cập, sử dụng, tiết lộ, làm gián đoạn, sửa đổi, làm sai lệch chức năng, phá hoại trái phép thông tin và hệ thống thông tin.

4. *Hạ tầng kỹ thuật* là tập hợp thiết bị tính toán (máy chủ, máy trạm), thiết bị ngoại vi, thiết bị kết nối mạng, thiết bị phụ trợ, mạng nội bộ, mạng diện rộng.

5. *Hệ thống thông tin* là tập hợp các thiết bị viễn thông, CNTT bao gồm phần cứng, phần mềm và cơ sở dữ liệu phục vụ cho hoạt động lưu trữ, xử lý, truyền tin, chia sẻ, trao đổi, cung cấp và sử dụng thông tin.

6. *Trang thông tin điện tử (website)* là hệ thống thông tin dùng để thiết lập một hoặc nhiều trang thông tin được trình bày dưới dạng ký hiệu, số, chữ viết, hình ảnh, âm thanh và các dạng thông tin khác phục vụ cho việc cung cấp và sử dụng thông tin trên Internet.

7. *Cổng thông tin điện tử (Portal)* là Trang thông tin điện tử tích hợp các kênh thông tin, các dịch vụ và ứng dụng theo một phương thức thống nhất, thông qua một điểm truy cập duy nhất đối với người sử dụng (từ nay gọi chung là website).

8. *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.

9. *Cổng giao tiếp (Port)* dùng để định danh các ứng dụng gửi và nhận dữ liệu, mỗi ứng dụng sẽ tương ứng với một cổng giao tiếp, những ứng dụng phổ biến được đặt với số hiệu cổng định trước, nhằm định danh duy nhất các ứng dụng đó. Khi máy tính sử dụng dịch vụ nào thì cổng giao tiếp tương ứng với dịch vụ đó sẽ mở.

10. *Bản ghi nhật ký hệ thống (Logfile)* là một tập tin được tạo ra trên mỗi thiết bị của hệ thống thông tin như: Tường lửa, máy chủ ứng dụng,... có chứa tất cả thông tin về các hoạt động xảy ra trên thiết bị đó. Bản ghi nhật ký hệ thống dùng để phân tích những sự kiện đã xảy ra, nguồn gốc và các kết quả để có các biện pháp xử lý thích hợp.

11. *TCVN 7562:2005:* Tiêu chuẩn Việt Nam về mã thực hành quản lý ATTT .

12. *ISO/IEC 17799:2005:* Tiêu chuẩn về CNTT - kỹ thuật an ninh - mã thực hành quản lý ATTT của Tổ chức Tiêu chuẩn quốc tế (ISO).

13. *ISO 27001:2005:* Tiêu chuẩn về CNTT - hệ thống quản lý an ninh thông tin của ISO.

Điều 3. Phạm vi và tài nguyên đảm bảo an toàn thông tin

1. Hệ thống mạng của Trường và các đơn vị trực thuộc Trường bao gồm:

a) Hệ thống máy chủ;

b) Hệ thống đường truyền dữ liệu, đường kết nối Internet;

c) Hệ thống mạng có dây, không dây;

d) Các trang thiết bị CNTT được kết nối mạng trong đơn vị.

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

a) Hệ thống thư điện tử;

b) Hệ thống cơ sở dữ liệu, phần mềm quản lý học phần tín chỉ ;

c) Cổng thông tin điện tử và hệ thống các website;

d) Các phần mềm ứng dụng phục vụ công tác quản lý, điều hành hoạt động của Nhà trường.

Điều 4. 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. Các dự án CNTT hoặc có cấu phần CNTT phải có ý kiến thẩm định chuyên môn về CNTT trong đó có thẩm định nội dung liên quan đến ATTT trước khi được phê duyệt.

3. 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.

Điều 5. 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. Tấn công, vô hiệu hóa trái phép làm mất tác dụng của biện pháp bảo vệ ATTT cho hệ thống thông tin; 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 (swich), 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.

Chương II

NỘI DUNG, BIỆN PHÁP BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 6. Lưu trữ và trao đổi thông tin

1. Việc lưu trữ và trao đổi thông tin phải tuân thủ các quy định của pháp luật về lưu trữ, CNTT và truyền thông.

2. Các dữ liệu, thông tin và tài liệu quan trọng, ở các mức độ mật, tối mật, tuyệt mật thì người sử dụng phải soạn thảo, lưu trữ tại máy tính riêng không kết nối mạng. Phải đặt mật khẩu, mã hoá dữ liệu và các biện pháp bảo mật khác đảm bảo an toàn, an ninh thông tin.

Điều 7. Yêu cầu về công tác bảo đảm an toàn thông tin

1. Hệ thống mạng nội bộ của Trường và các đơn vị trực thuộc phải được trang bị hệ thống kỹ thuật, công nghệ hiện đại; 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 virus tin học, thư rác cho hệ thống thư điện tử, máy chủ, máy trạm trong các đơn vị.

2. Có biện pháp bảo vệ, phòng và chống các nguy cơ mất cắp thông tin, cháy nổ, ngập dột 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 (khóa, thẻ nhận dạng,...) cho phù hợp đối với cán bộ, viên chức đã nghỉ việc hoặc chuyển công tác.

5. Hệ thống thông tin quản lý, hệ thống cơ sở dữ liệu, hệ thống máy chủ phải có chức năng tự động ghi nhật ký (trong khoảng thời gian nhất định, tối thiểu là 3 tháng) quá trình đăng nhập vào hệ thống, các thao tác cấu hình hệ thống và các thông tin liên quan về ATTT để phục vụ công tác khắc phục sự cố và điều tra về ATTT khi xảy ra.

6. Việc thanh lý, tiêu huỷ thiết bị hoặc vật mang thông tin (đĩa cứng, đĩa di động,...) phải đảm bảo yêu cầu không để lộ, lọt thông tin nhà nước. Phải có quy trình cụ thể và phải lưu giữ hồ sơ, biên bản thanh lý, tiêu hủy.

Điều 8. Biện pháp quản lý vận hành đảm bảo an toàn thông tin

1. Đối với cán bộ phụ trách ATTT tại các đơn vị thuộc Trường:

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 ATTT, 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.

d) Thường xuyên thực hiện việc theo dõi bản ghi nhật ký hệ thống và các sự kiện khác có liên quan để đánh giá, báo cáo mức độ nghiêm trọng các rủi ro đó. Các rủi ro đó có thể xảy ra do sự truy cập trái phép, sử dụng trái phép, mất, thay đổi hoặc phá hủy thông tin và hệ thống thông tin.

đ) Kiểm soát chặt chẽ việc cài đặt phần mềm vào máy trạm và máy chủ.

3. Đối với cán bộ, viên chức, người lao động:

a) Thường xuyên cập nhật những chính sách, thủ tục ATTT của cơ quan, đơn vị và thực hiện đúng hướng dẫn về ATTT của cán bộ phụ trách.

b) Thực hiện quét virus 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 virus, 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 virus, phần mềm gián điệp xâm nhập máy tính phá hoại, đánh cắp thông tin. Định kỳ thường xuyên quét virus, phần mềm gián điệp trên máy tính.

Điều 9. Biện pháp quản lý kỹ thuật đảm bảo an toàn thông tin

1. 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: mật khẩu, cấp phép truy cập đối với địa chỉ vật lý (MAC address), mã hóa dữ liệu và thông báo các thông tin liên quan đến điểm truy nhập để cơ quan sử dụng, thường xuyên thay đổi mật khẩu nhằm tăng cường công tác bảo mật.

3. Quản lý đăng nhập hệ thống:

a) Các hệ thống thông tin cần giới hạn một số hữu hạn lần đăng nhập sai liên tiếp. Nếu liên tục đăng nhập sai vượt quá số lần quy định, hệ thống phải tự động

khóa tài khoản hoặc cô lập tài khoản trong một khoảng thời gian nhất định trước khi tiếp tục cho đăng nhập. 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.

b) Tổ chức theo dõi, kiểm soát tất cả các phương pháp truy nhập từ xa (quay số, Internet,...) tới hệ thống thông tin, bao gồm cả sự truy nhập có chức năng quản trị, tăng cường sử dụng mạng riêng ảo khi có nhu cầu làm việc từ xa; 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.

c) 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, virus:

Lựa chọn, triển khai các phần mềm chống virus, thư rác có hiệu quả trên máy chủ, máy trạm, các thiết bị, phương tiện kỹ thuật trong mạng, các hệ thống thông tin như: Cổng/Trang thông tin điện tử, thư 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 (virus, trojan, worms,..).

5. Tổ chức quản lý tài nguyên:

Kiểm tra, giám sát chức năng chia sẻ thông tin. Tổ chức cấp phát tài nguyên trên máy chủ theo danh mục thư mục cho từng đơn vị; khuyến cáo người sử dụng cân nhắc việc chia sẻ tài nguyên cục bộ trên máy đang sử dụng, khi thực hiện việc chia sẻ tài nguyên cần phải sử dụng mật khẩu để bảo vệ thông tin.

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

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

- Luôn cập nhật bản vá lỗi mới nhất cho hệ quản trị cơ sở dữ liệu; sử dụng công cụ để đánh giá, tìm kiếm lỗ hổng trên máy chủ cơ sở dữ liệu;

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

- Có cơ chế sao lưu dữ liệu, tài liệu hóa quá trình thay đổi cấu trúc bằng cách xây dựng nhật ký cơ sở dữ liệu với các nội dung như: Nội dung thay đổi, lý do thay đổi, thời gian, vị trí thay đổi.

b) Phối hợp với công ty phần mềm PSC 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.

7. 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.

8. 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.

9. Hệ thống thông tin tại các đơn vị cần có cơ chế ngăn chặn hoặc hạn chế các sự cố gây ra do tấn công từ chối dịch vụ (DoS, DDoS). Sử dụng các thiết bị đặt tại biên của mạng để lọc các gói tin nhằm bảo vệ các thiết bị bên trong, tránh bị ảnh hưởng trực tiếp bởi tấn công từ chối dịch vụ.

Điều 10. Xây dựng quy chế nội bộ đảm bảo an toàn thông tin

1. Các đơn vị phải ban hành hoặc điều chỉnh, bổ sung quy chế nội bộ, đảm bảo quy định rõ các vấn đề sau:

a) Mục tiêu và phương hướng thực hiện công tác đảm bảo an toàn, an ninh cho hệ thống thông tin.

b) Nguyên tắc phân loại và quản lý mức độ ưu tiên đối với các tài nguyên của hệ thống thông tin (phần mềm, dữ liệu, trang thiết bị).

c) Quản lý phân quyền và trách nhiệm đối với từng cá nhân khi tham gia sử dụng hệ thống thông tin.

d) Quản lý và điều hành hệ thống máy chủ, thiết bị mạng, thiết bị bảo vệ mạng một cách an toàn.

đ) Kiểm tra, khắc phục sự cố an toàn, an ninh của hệ thống thông tin bằng cách sử dụng các biện pháp tại Quy chế này.

e) Nguyên tắc chung về sử dụng an toàn và hiệu quả đối với các cá nhân tham gia sử dụng hệ thống thông tin.

g) Báo cáo tình hình an toàn, an ninh hệ thống thông tin theo định kỳ.

2. Các đơn vị xây dựng quy chế ATTT cần căn cứ các tiêu chuẩn kỹ thuật quản lý an toàn của Bộ tiêu chuẩn TCVN 7562:2005 và ISO/IEC 17799:2005 tại Phụ lục I kèm theo Quy chế này, để áp dụng cho phù hợp.

Điều 11. Xây dựng và áp dụng quy trình đảm bảo an toàn thông tin

1. Các đơn vị phải xây dựng và áp dụng quy trình đảm bảo an toàn, an ninh cho hệ thống thông tin nhằm giảm thiểu các nguy cơ gây ra sự cố, tạo điều kiện cho việc khắc phục và truy vết trong trường hợp có sự cố xảy ra. Nội dung của quy trình có thể chia làm các bước cơ bản như:

a) Lập kế hoạch bảo vệ an toàn, an ninh cho hệ thống thông tin.

b) Xây dựng hệ thống bảo vệ ATTT.

c) Quản lý và vận hành hệ thống bảo vệ ATTT.

d) Kiểm tra đánh giá hoạt động của hệ thống bảo vệ ATTT.

đ) Bảo trì và nâng cấp hệ thống bảo vệ ATTT.

2. Các đơn vị tham khảo các bước cơ bản để xây dựng khung quy trình đảm bảo ATTT cho hệ thống thông tin tại Phụ lục II - Các bước cơ bản để xây dựng khung quy trình đảm bảo ATTT và Phụ lục I - Những nội dung chính của ISO 17799:2005 dùng để xây dựng quy chế nội bộ đảm bảo ATTT cho hệ thống thông tin kèm theo Quy chế này.

Chương III
TỔ CHỨC THỰC HIỆN

Điều 12. Trách nhiệm của trưởng các đơn vị

1. Đảm bảo ATTT cho các hệ thống CNTT thuộc đơn vị quản lý, vận hành.

2. Tuyên truyền, nâng cao nhận thức cho viên chức và người lao động về các nguy cơ mất ATTT; tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trước Hiệu trưởng trong công tác đảm bảo ATTT của đơn vị.

3. Khi có sự cố hoặc có nguy cơ mất ATTT phải kịp thời chỉ đạo khắc phục. Trường hợp không khắc phục được thì phối hợp với cán bộ CNTT để được hướng dẫn, hỗ trợ.

Điều 13. Trách nhiệm của viên chức và người lao động

1. Trách nhiệm của cán bộ phụ trách ATTT:

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.

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 ATTT .

2. Trách nhiệm của viên chức và người lao động:

a) Chấp hành nghiêm túc các quy định về ATTT của cơ quan, đơn vị, của Quy chế 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 ATTT để kịp thời ngăn chặn, xử lý.

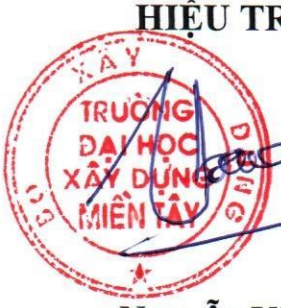
c) Tích cực tham gia các chương trình đào tạo, hội nghị về ATTT do Bộ GDĐT hoặc các đơn vị chuyên môn tổ chức.

Điều 14. Xử lý vi phạm

Các đơn vị, cá nhân có hành vi vi phạm Quy chế này, tùy theo tính chất, mức độ vi phạm mà bị xử lý theo quy định của pháp luật./.

Nơi nhận:
- BGH;
- Như Điều 1;
- Website trường;
- Lưu: VT, QLĐT.

HIỆU TRƯỞNG



Nguyễn Văn Xuân