BỘ LAO ĐỘNG - THƯƠNG BINH VÀ XÃ HỘI
TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT VĨNH LONG

Số: 13 /QĐ-ĐHSPKTVL

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

Vĩnh Long, ngày 15 tháng 02 năm 2017

QUYẾT ĐỊNH

Về việc ban hành Quy định đảm bảo an toàn, bảo mật thông tin về đảm bảo chất lượng bên trong thuộc lĩnh vực công nghệ thông tin tại Trường Đại học Sư phạm Kỹ thuật Vĩnh Long

HIỆU TRƯỞNG TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT VĨNH LONG

Căn cứ quyết định số 1785/QĐ – LĐTBXH, ngày 21/11/2013 của Bộ trưởng Bộ Lao động – Thương binh và Xã hội về việc Quy định chức năng, nhiệm vụ và cơ cấu tổ chức của trường Trường Đại học Sư phạm Kỹ thuật Vĩnh Long;

Căn cứ Nghị định số 72/2013/NĐ-CP, ngày 15/7/2013 của Chính phủ về quản lý, cung cấp và sử dụng dịch vụ Internet và thông tin trên mạng;

Căn cứ Thông tư số 23/2011/TT-BTTTT Quy định về việc quản lý, vận hành, sử dụng và bảo đảm an toàn thông tin trên Mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước;

Căn cứ Quyết định 63/QĐ-TTg ngày 13/01/2010 của Thủ tướng Chính phủ về việc phê duyệt Quy hoạch phát triển an toàn thông tin số quốc gia đến năm 2020;

Xét đề nghị của Trưởng phòng Khảo thí và Đảm bảo chất lượng giáo dục,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này là Quy định đảm bảo an toàn, bảo mật thông tin về đảm bảo chất lượng bên trong thuộc lĩnh vực công nghệ thông tin tại Trường Đại học Sư phạm Kỹ thuật Vĩnh Long;

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

Điều 3. Phòng Khảo thí & Đảm bảo chất lượng giáo dục, các đơn vị phòng, khoa, bộ môn trung tâm và toàn thể cán bộ, công chức, viên chức trong Trường chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Lưu VT.

HIỆU TRƯỞNG

BỘ LAO ĐỘNG THƯƠNG BINH VÀ XÃ HỘI
TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT VĨNH LONG

PGS.TS. Cao Hùng Phi

BỘ LAO ĐỘNG - THƯƠNG BINH VÀ XÃ HỘI
TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT VĨNH LONG

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

QUY ĐỊNH

Đảm bảo an toàn, bảo mật thông tin về đảm bảo chất lượng bên trong thuộc lĩnh vực công nghệ thông tin tại Trường Đại học Sư phạm Kỹ thuật Vĩnh Long

(Kèm theo Quyết định số 13 / QĐ-ĐHSPKTVL ngày 15 tháng 02 năm 2017 của Hiệu trưởng Trường Đại học Sư phạm kỹ thuật Vĩnh Long)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi

Quy định này quy định các nội dung của công tác đảm bảo an toàn, bảo mật thông tin về đảm bảo chất lượng bên trong thuộc trong hoạt động ứng dụng công nghệ thông tin tại các đơn vị phòng, khoa, bộ môn, trung tâm thuộc trường Đại học Sư phạm Kỹ thuật Vĩnh Long, bao gồm: công tác xây dựng các quy định quản lý đảm bảo an toàn, bảo mật thông tin; việc áp dụng các biện pháp quản lý kỹ thuật, quản lý vận hành đảm bảo an toàn, bảo mật thông tin đối với hệ thống thông tin.

Điều 2. Đối tượng áp dụng

1. Quy định này được áp dụng đối với các đơn vị phòng, khoa, bộ môn, trung tâm thuộc trường Đại học Sư phạm Kỹ thuật Vĩnh Long.

2. Cán bộ, công chức, viên chức đang làm việc tại Khoản 1 điều này; Những tổ chức, cá nhân có liên quan áp dụng Quy định này trong việc vận hành, khai thác và sử dụng hệ thống thông tin tại Trường.

Điều 3. Giải thích từ ngữ

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

1. Tính tin cậy: Đảm bảo thông tin chỉ có thể được truy cập bởi những người được cấp quyền sử dụng.

2. Tính toàn vẹn: Bảo vệ tính chính xác và tính đầy đủ của thông tin và các phương pháp xử lý thông tin.

3. Tính sẵn sàng: Đảm bảo những người được cấp quyền có thể truy cập thông tin và các tài sản liên quan ngay khi có nhu cầu.

Chương II
QUY ĐỊNH ĐẢM BẢO AN TOÀN, BẢO MẬT THÔNG TIN

Điều 4. Các biện pháp quản lý vận hành trong công tác đảm bảo an toàn, bảo mật thông tin

1. Các cán bộ, công chức, viên chức phải trang bị đầy đủ các kiến thức bảo mật cơ bản trước khi cho phép truy cập và sử dụng hệ thống thông tin.

2. Phải bố trí cán bộ phụ trách về an toàn, bảo mật thông tin (sau đây gọi tắt là cán bộ phụ trách). Cán bộ phụ trách được đảm bảo điều kiện học tập, tiếp thu công nghệ, kiến thức an toàn bảo mật thông tin trước khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ.

3. Cán bộ phụ trách phải thường xuyên cập nhật cấu hình chuẩn cho các thành phần của hệ thống thông tin, thiết lập cấu hình một cách chặt chẽ nhất cho các sản phẩm an toàn thông tin nhưng vẫn đảm bảo duy trì hoạt động thường xuyên của hệ thống thông tin.

4. Cán bộ phụ trách phải tổ chức cấu hình hệ thống thông tin chỉ cung cấp những chức năng thiết yếu nhất, đồng thời xác định các chức năng, cổng giao tiếp mạng, giao thức và dịch vụ không cần thiết để cấm hoặc hạn định sử dụng.

5. Hệ thống thông tin tại các đơn vị phòng, khoa, bộ môn, trung tâm... phải có cơ định sao lưu thông tin ở mức người dùng và mức hệ thống (bao gồm: sao lưu trạng thái hệ thống thông tin và lưu trữ thông tin sao lưu tại nơi an toàn), đồng thời thông tin sao lưu phải được tổ chức kiểm tra thường xuyên để đảm bảo tính sẵn sàng và toàn vẹn thông tin.

6. Hệ thống thông tin phải được triển khai cơ định chống virus, thư rác cho những hệ thống xung yếu hiện hữu (firewall, mail server,...) và tại các máy trạm, máy chủ trong mạng; tổ chức sử dụng cơ định chống virus, thư rác để phát hiện và loại trừ những đoạn mã độc hại (virus, trojan, worms...) có khả năng khai thác các lỗ hổng của hệ thống thông tin, được truyền tải bởi thư điện tử, tập tin đính kèm từ Internet, thiết bị lưu trữ tháo lắp; đồng thời thường xuyên cập nhật cơ định chống virus, thư rác phù hợp với quy trình và chính sách quản lý cấu hình hệ thống thông tin của cơ quan, đơn vị.

7. Cán bộ phụ trách phải thường xuyên thực hiện đánh giá, báo cáo các rủi ro và mức độ nghiêm trọng của các rủi ro đó. Các rủi ro có thể xảy ra do nguy cơ tự nhiên, truy cập trái phép, sử dụng trái phép dẫn đến làm mất, thay đổi hoặc phá hủy thông tin và hệ thống thông tin.

8. Đối với cán bộ, công chức, viên chức đã nghỉ việc, các đơn vị phòng, khoa, bộ môn, trung tâm phải thực hiện hủy quyền truy cập hệ thống thông tin và thu hồi các tài sản liên quan nhưng vẫn đảm bảo khả năng truy cập vào các hồ sơ được tạo ra bởi cán bộ, công chức hoặc nhân viên đó.

9. Thường xuyên quan tâm phân bổ đầu tư cần thiết để đảm bảo và tăng cường an toàn, bảo mật thông tin trong hoạt động ứng dụng công nghệ thông tin của từng đơn vị.

Điều 5. Các biện pháp quản lý kỹ thuật cho công tác đảm bảo an toàn, bảo mật thông tin

1. Biện pháp an toàn đối với hệ thống thông tin

a. Tổ chức quản lý các tài khoản của hệ thống thông tin, bao gồm: Tạo mới, kích hoạt, sửa đổi, vô hiệu hóa và loại bỏ các tài khoản, đồng thời tổ chức kiểm tra các tài khoản của hệ thống thông tin ít nhất 01 lần/01 năm đối với tài khoản người dùng thông thường và 03 tháng/1 lần đối với tài khoản quản trị. Triển khai các công cụ tự động để hỗ trợ việc quản lý các tài khoản của hệ thống thông tin.

b. Hệ thống thông tin phải có cơ định giới hạn một số hữu hạn lần đăng nhập sai liên tiếp. Nếu liên tục đăng nhập sai vượt quá số lần quy định thì hệ thống sẽ tự động khóa hoặc cô lập tài khoản trong một khoảng thời gian nhất định trước khi tiếp tục cho đăng nhập.

c. Cán bộ phụ trách có trách nhiệm tổ chức theo dõi và kiểm soát tất cả các phương pháp truy cập từ xa tới hệ thống thông tin, bao gồm cả sự truy cập có chức năng đặc quyền. Hệ thống thông tin tại phải có cơ định kiểm tra, cho phép tương ứng với mỗi phương pháp truy cập từ xa và cơ định tự động giám sát, điều khiển các truy cập từ xa.

d. Cán bộ phụ trách phải thiết lập phương pháp hạn định truy cập mạng không dây, giám sát và điều khiển truy cập không dây, tổ chức sử dụng chứng thực và mã hóa để bảo vệ truy cập không dây tới hệ thống thông tin.

e. Hệ thống thông tin phải ghi nhận được các sự kiện về quá trình đăng nhập hệ thống, các thao tác cấu hình hệ thống, quá trình truy xuất hệ thống, đồng thời ghi nhận đầy đủ các thông tin liên quan vào các bản ghi nhật ký nhằm xác định những sự kiện nào đã xảy ra, nguồn gốc và các kết quả của sự kiện đó để có cơ định bảo vệ và lưu giữ nhật ký trong một khoảng thời gian nhất định.

f. Cán bộ phụ trách phải tổ chức quản lý định danh đối với tất cả người dùng tham gia sử dụng hệ thống thông tin.

2. Biện pháp bảo mật đối với thông tin

a. Đánh nhãn các thiết bị lưu trữ, tài liệu trên giấy tờ: Tùy nhãn của chúng mà được lưu trữ trong những khu vực khác nhau.

b. Sử dụng, truy xuất các thiết bị lưu trữ: USB, Đĩa Mềm, CD/DVD/BlueRay.

- Thông tin bình thường: có thể tùy ý sử dụng.

- Thông tin nhay cảm: Cần phải có sự đồng ý của cấp trên mới có thể sử dụng hay mang ra ngoài.

- Thông tin mật: Cần được xác nhận của Phó Hiệu trưởng trở lên.

- Thông tin tuyệt mật: Chỉ có Hiệu trưởng mới có thể quyết định.

c. Hủy dữ liệu trong các thiết bị: USB, Đĩa Mềm, CD, Băng Từ, HDD

- Thông tin bình thường: Xóa bình thường, không bắt buộc phải format.

- Thông tin nhạy cảm: Thiết bị lưu trữ cần được format lại.

- Thông tin mật: Phải ghi đè nhiều lần đảm bảo không thể khôi phục lại.

- Thông tin tuyệt mật: Hủy cả dữ liệu lẫn thiết bị.

d. Đối với các hồ sơ, văn bản giấy thực hiện việc bảo đảm an toàn, bảo mật thông tin theo tiêu chuẩn ISO.

Điều 6. Nhiệm vụ của các đơn vị

1. Phòng Khảo thí & Đảm bảo chất lượng giáo dục

Xây dựng và áp dụng quy trình đảm bảo an toàn, bảo mật thông tin: Phòng khảo thí và Đảm bảo chất lượng giáo dục xây dựng và áp dụng quy trình đảm bảo an toàn, bảo mật thông tin cho hệ thống thông tin của mình nhằm giảm thiểu các nguy cơ gây sự cố, tạo điều kiện cho việc khắc phục và truy vết trong trường hợp có sự cố xảy ra.

2. Phòng Quản trị - Thiết bị

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

b. Kiểm tra, rà soát và khắc phục sự cố mất an toàn, bảo mật thông tin của hệ thống bằng cách sử dụng các biện pháp trong Điều 4 và Điều 5 của Quy định này;

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

d. Áp dụng quy trình bảo vệ an toàn, bảo mật thông tin:

- Lập kế hoạch bảo vệ an toàn, bảo mật thông tin cho hệ thống thông tin;
- Xây dựng hệ thống bảo vệ an toàn, bảo mật thông tin;
- Quản lý và vận hành hệ thống bảo vệ an toàn, bảo mật thông tin;
- Kiểm tra đánh giá hoạt động hệ thống bảo vệ an toàn, bảo mật thông tin;
- Bảo trì và nâng cấp hệ thống bảo vệ an toàn, bảo mật thông tin.

3. Khoa Công nghệ thông tin

Tư vấn giải pháp an toàn, bảo mật thông tin, phối hợp hỗ trợ kỹ thuật với các đơn vị liên quan khi có sự cố.

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN, BẢO MẬT THÔNG TIN

Điều 7. Trách nhiệm

1. Phòng Khảo thí & Đảm bảo chất lượng giáo dục

a. Tham mưu cho Hiệu trưởng về công tác đảm bảo an toàn, bảo mật thông tin đảm bảo chất lượng.

b. Báo cáo tình hình và kết quả thực hiện công tác đảm bảo an toàn, bảo mật thông tin khi có yêu cầu.

c. Thực hiện nghiêm túc các quy định tại Quy định này.

2. Phòng Quản trị - Thiết bị

a. Khi có sự cố hoặc nguy cơ mất an toàn, bảo mật thông tin phải kịp thời áp dụng mọi biện pháp để khắc phục và hạn định thiệt hại, ưu tiên sử dụng lực lượng kỹ thuật an toàn thông tin của Trường, lập biên bản, báo cáo bằng văn bản cho Hiệu trưởng.

b. Tạo điều kiện thuận lợi cho các cơ quan chức năng tham gia khắc phục sự cố và thực hiện đúng theo hướng dẫn.

c. Hướng dẫn, giám sát công tác xây dựng và áp dụng quy định về quản lý an toàn, bảo mật thông tin cho các đơn vị phòng, khoa, bộ môn, trung tâm trong Trường.

d. Báo cáo tình hình và kết quả thực hiện công tác đảm bảo an toàn, bảo mật thông tin khi có yêu cầu.

e. Thực hiện nghiêm túc các quy định tại Quy định này.

Điều 8. Trách nhiệm của trưởng các đơn vị phòng, khoa, bộ môn, trung tâm, cán bộ, công chức, viên chức trong Trường.

1. Trách nhiệm của trưởng các đơn vị: Trưởng các đơn vị trong Trường có trách nhiệm đôn đốc, kiểm tra cán bộ, công chức, viên chức thuộc đơn vị mình quản lý tuân thủ nghiêm túc các quy định tại Quy định này.

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

a) Nghiêm chỉnh thi hành các quy định nội bộ, quy trình về an toàn, bảo mật thông tin của Trường cũng như các quy định khác của pháp luật, nâng cao ý thức cảnh giác, trách nhiệm đảm bảo an toàn, bảo mật thông tinh.

b) Khi phát hiện sự cố phải báo cáo ngay với cấp trên và phòng Khảo thí và Đảm bảo chất lượng giáo dục và phòng Quản trị - Thiết bị để kịp thời ngăn chặn, xử lý.

Điều 9. Kế hoạch kiểm tra hàng năm.

1. Phòng Khảo thí và Đảm bảo chất lượng giáo dục chủ trì, phối hợp với phòng Quản trị - Thiết bị tiến hành kiểm tra công tác đảm bảo an toàn, bảo mật thông tin theo định kỳ.

2. Phối hợp với các đơn vị liên quan thực hiện việc kiểm tra đột xuất các đơn vị phòng, khoa, bộ môn, trung tâm và cá nhân khi có dấu hiệu vi phạm an toàn, bảo mật thông tin trong hệ thống thông tin.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 10. Tổ chức thực hiện.

1. Phòng Khảo thí và Đảm bảo chất lượng giáo dục chủ trì, phối hợp với các đơn vị phòng, khoa, bộ môn, trung tâm và các cơ quan tổ chức có liên quan triển khai thực hiện Quy định này.

2. Tổ chức, cá nhân có hành vi vi phạm Quy định này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật theo trách nhiệm, xử phạt hành chính hoặc bị truy cứu trách nhiệm hình sự. Nếu gây thiệt hại thì phải bồi thường theo quy định hiện hành của pháp luật./.

HIỆU TRƯỞNG

BỘ LAO ĐỘNG THƯƠNG BINH VÀ XÃ HỘI
TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT VĨNH LONG

PGS.TS. Cao Hùng Phi