ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

Số: 887/QĐ-ĐHKH

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

Thái Nguyên, ngày 30 tháng 11 năm 2015

QUYẾT ĐỊNH

Ban hành quy chế bảo mật, bảo đảm an toàn, an ninh thông tin mạng trường Đại học Khoa học

HIỆU TRƯỞNG TRƯỜNG ĐẠI HỌC KHOA HỌC

Căn cứ Quyết định số 1901/QĐ-TTg ngày 23/12/2008 của Thủ tướng Chính phủ về việc thành lập trường Đại học Khoa học trực thuộc Đại học Thái Nguyên;

Căn cứ Thông tư số 08/2014/TT-BGDĐT ngày 20/3/2014 của Bộ trưởng Bộ Giáo dục và Đào tạo ban hành Quy chế tổ chức và hoạt động của đại học vùng và các cơ sở giáo dục thành viên;

Căn cứ Quyết định số 1245/QĐ-ĐHTN ngày 03/11/2011 của Giám đốc Đại học Thái Nguyên về việc ban hành quy định về phân cấp quản lý công tác tổ chức bộ máy cho các trường đại học, cao đẳng thuộc Đại học Thái Nguyên;

Căn cứ Quyết định số 281/QĐ-ĐHTN ngày 03/4/2012 của Giám đốc Đại học Thái Nguyên về việc thành lập Trung tâm CNTT-TV thuộc trường Đại học Khoa học;

Căn cứ Quyết định số 77/QĐ-ĐHKH ngày 30/01/2015 của Hiệu trưởng trường Đại học Khoa học về việc ban hành quy định chức năng nhiệm vụ Trung tâm CNTT-TV trường Đại học Khoa học;

Xét đề nghị của Giám đốc Trung tâm CNTT-TV,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này "Quy chế bảo mật, bảo đảm an toàn, an ninh thông tin mạng trường Đại học Khoa học".

Điều 2. Quyết định này có hiệu lực kể từ ngày 01/12/2015.

Điều 3. Các ông (bà) Giám đốc Trung tâm CNTT-TV, Thủ trưởng các đơn vị có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Ban Giám hiệu;
- Các đơn vị;
- Website, eDocman;
- Lưu: VT, TT CNTT-TV

HIỆU TRƯỞNG

TRƯỜNG ĐẠI HỌC KHOA HỌC

PGS.TS. Nông Quốc Chinh

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

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

Thái Nguyên, ngày tháng năm 2015

QUY CHẾ
Bảo mật, đảm bảo an toàn, an ninh thông tin mạng trường Đại học Khoa học

(Ban hành kèm theo Quyết định số: 887/QĐ-ĐHKH ngày 30 /11 /2015)

Chương I
NHỮNG QUY ĐỊNH CHUNG

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

1. Quy chế này quy định việc bảo mật, bảo đảm an toàn, an ninh thông tin mạng của trường Đại học Khoa học.

2. Quy chế này áp dụng đối với các đơn vị, tổ chức thuộc trường Đại học Khoa học; cán bộ, công chức, viên chức, HSSV, học viên, NCS khai thác, sử dụng mạng và tài nguyên mạng của trường Đại học Khoa học.

Điều 2. Giải thích từ ngữ

1. Mạng trường Đại học Khoa học: Là hệ thống mạng thông tin của trường Đại học Khoa học, có mở rộng tới các đơn vị, tổ chức trong Nhà trường.

2. Người sử dụng: Là những cá nhân, tổ chức được quyền khai thác, sử dụng tài nguyên mạng trường Đại học Khoa học.

3. Đảm bảo an toàn thông tin: Là các hoạt động nghiệp vụ và kỹ thuật nhằm bảo vệ, khôi phục các hệ thống, các dịch vụ và nội dung thông tin đối với các nguy cơ khách quan hoặc do con người gây ra, bảo đảm cho các hệ thống thực hiện đúng chức năng, thông tin được bảo mật, toàn vẹn, sẵn sàng, chính xác và tin cậy.

4. Thông tin điện tử: Là các thông tin được lưu trữ, kết nối và truyền tải trong mạng trường Đại học Khoa học.

5. Hệ thống giám sát an ninh mạng: Là tập hợp các thiết bị công nghệ thông tin hoạt động theo một chính sách an ninh nhất quán nhằm quản lý, giám sát chặt chẽ mọi luồng thông tin trong hệ thống mạng, phát hiện và ngăn chặn các truy cập trái phép nhằm thay đổi hoặc phá hoại nội dung thông tin.

Điều 3. Phạm vi và tài nguyên mạng trường Đại học Khoa học

1. Phạm vi mạng trường Đại học Khoa học bao gồm:

a) Hệ thống mạng nội bộ (LAN), mạng diện rộng (WAN);

b) Hệ thống mạng kết nối Internet;

2. Tài nguyên mạng trường Đại học Khoa học bao gồm:

a) Hệ thống địa chỉ sử dụng để giao tiếp trong mạng trường Đại học Khoa học;

b) Các trang thiết bị công nghệ thông tin kết nối vào mạng trường Đại học Khoa học;

c) Các cơ sở dữ liệu và các tệp tin dữ liệu;

d) Hệ thống thư điện tử;

đ) Các phần mềm hệ thống, phần mềm ứng dụng phục vụ công tác quản lý, điều hành hoạt động trong mạng trường Đại học Khoa học;

e) Cổng thông tin điện tử của trường Đại học Khoa học; trang thông tin điện tử của các đơn vị thuộc và trực thuộc trường Đại học Khoa học;

g) Các thông tin được xử lý, truyền tải, lưu trữ trong mạng trường Đại học Khoa học.

Điều 4. Ngôn ngữ trao đổi trong mạng trường Đại học Khoa học

Ngôn ngữ được dùng để trao đổi thông tin trong mạng trường Đại học Khoa học sử dụng bộ mã các ký tự chữ Việt theo tiêu chuẩn TCVN 6909:2001 được quy định tại Quyết định số 72/2002/QĐ-TTg ngày 10/6/2002 của Thủ tướng Chính phủ.

Chương II

NỘI DUNG BẢO MẬT, BẢO ĐẢM AN TOÀN, AN NINH THÔNG TIN MẠNG TRƯỜNG ĐẠI HỌC KHOA HỌC

Điều 5. Lưu trữ và trao đổi thông tin trong mạng trường Đại học Khoa học

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

2. Các thông tin bị cấm lưu trữ, trao đổi trong mạng Trường Đại học Khoa học và đưa lên Cổng thông tin điện tử Trường Đại học Khoa học hoặc trang thông tin điện tử của các đơn vị thuộc trường Đại học Khoa học:

a) Thông tin chưa được cấp có thẩm quyền cho phép công bố;

b) Thông tin thuộc danh mục thông tin mật do pháp luật hiện hành quy định; các thông tin mật của Trường, các thông tin lưu hành nội bộ.

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

- Làm ảnh hưởng đến an ninh quốc gia;

- Xuyên tạc, tuyên truyền chống đối các chủ trương, đường lối của Đảng chính sách và pháp luật của Nhà nước, phá hoại khối đại đoàn kết dân tộc;

- 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 xấu đến đời tư công dân: Các thông tin quấy rối cá nhân, xúc phạm danh dự, vu khống, xúc phạm đến nhân phẩm công dân;

- Có ảnh hưởng xấu đến an ninh kinh tế: Thông tin lừa đảo, thông tin bí mật kinh tế;

- Vi phạm quyền sở hữu trí tuệ: Sử dụng và truyền bá trái phép các sản phẩm có bản quyền, phần mềm tin học, tác phẩm nghệ thuật được pháp luật bảo hộ;

- Có ảnh hưởng xấu đến bảo mật, an toàn thông tin: Các ứng dụng có tính chất phá hoại như vi rút tin học, lấy cắp thông tin, phá hoại cơ sở dữ liệu, làm tê liệt mạng trường Đại học Khoa học;

- Có ảnh hưởng xấu đến văn hóa xã hội: Xuyên tạc lịch sử, phủ nhận các thành quả cách mạng, xúc phạm các vĩ nhân và các anh hùng dân tộc, phao tin đồn gây ảnh hưởng đến uy tín của quốc gia;

- Trái với thuần phong mỹ tục: Tệ nạn xã hội, sử dụng các từ ngữ có nội dung không lành mạnh, thiếu văn hóa, các thông tin ảnh hưởng đến quyền tự do tín ngưỡng của công dân.

Điều 6. Yêu cầu về công tác bảo mật, bảo đảm an toàn, an ninh thông tin trong mạng trường Đại học Khoa học

1. Hệ thống thông tin trong mạng trường Đại học Khoa học được thiết kế thống nhất, cùng kết hợp và hỗ trợ, tương tác hoạt động với nhau, được tổ chức quản lý định danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý hệ thống chặt chẽ, bảo đảm an toàn và bảo mật.

2. Người sử dụng mạng trường Đại học Khoa học phải đăng ký sử dụng. Khi được phép sử dụng sẽ được cấp thông tin về tài khoản, mật khẩu truy cập và quyền khai thác, sử dụng tài nguyên mạng trường Đại học Khoa học.

3. Hệ thống mạng trường Đại học Khoa học phải được trang bị hệ thống kỹ thuật, công nghệ hiện đại để thường xuyên, liên tục quản lý, giám sát, kiểm soát mạng nhằm phát hiện, ngăn chặn các truy cập trái phép của người sử dụng, tin tặc tấn công mạng trường Đại học Khoa học; triển khai cơ chế phòng chống vi rút tin học, thư rác cho những hệ thống xung yếu (máy chủ thư điện tử, máy chủ website, máy chủ tên miền, v.v...) và tại các máy chủ, máy trạm khác trong hệ thống mạng trường Đại học Khoa học.

4. Có biện pháp bảo vệ, dự phòng, phòng chống các nguy cơ do mất cắp, cháy nổ, ngập lụt, động đất và các thảm họa khác do thiên nhiên hoặc con người gây ra và các phương án khôi phục hệ thống sau thảm họa.

5. Các dữ liệu, thông tin và tài liệu quan trọng, ở các mức độ mật thì người sử dụng phải soạn thảo, lưu trữ tại máy tính riêng không được kết nối vào mạng trường Đại học Khoa học và mạng Internet, phải đặt mật khẩu, mã hóa dữ liệu, sử dụng chứng thư số để bảo mật, bảo đảm an toàn, an ninh thông tin.

6. Xây dựng hệ thống dự phòng cho các hệ thống công nghệ thông tin. Phải có quy trình phục hồi, sao lưu định kỳ cho hệ thống, các phần mềm ứng dụng và các hệ thống cơ sở dữ liệu.

7. Tổ chức quản lý các tài khoản của hệ thống thông tin, bao gồm: Tạo mới, kích hoạt, sửa đổi, vô hiệu hóa và xóa bỏ các tài khoản; tổ chức kiểm tra các tài khoản của hệ thống thông tin ít nhất mỗi tháng 01 lần và triển khai các công cụ tự động để hỗ trợ việc quản lý các tài khoản của hệ thống thông tin.

8. Hệ thống thông tin phải có cơ chế giới hạn số lần đăng nhập sai liên tiếp, nếu đăng nhập sai vượt quá số lần quy định thì tài khoản sẽ tự động bị khóa.

9. Hệ thống thông tin phải có khả năng tự động ghi nhận được lịch sử quá trình đăng nhập hệ thống, các thao tác cấu hình hệ thống, quá trình truy xuất hệ thống và các thông tin liên quan đến an toàn, an ninh thông tin vào các bản ghi nhật ký.

10. Việc thanh lý, tiêu hủy thiết bị, vật mang thông tin trong mạng trường Đại học Khoa học 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 việc thanh lý, tiêu hủy.

Chương III
TỔ CHỨC THỰC HIỆN

Điều 7. Trách nhiệm của Trung tâm Công nghệ Thông tin – Thư viện (CNTT-TV)

1. Trung tâm CNTT-TV là đơn vị chuyên trách về công nghệ thông tin; thống nhất quản lý hoạt động, phối hợp với các cơ quan, đơn vị chức năng để đảm bảo thực thi công tác bảo mật, bảo đảm an toàn, an ninh thông tin trong mạng trường Đại học Khoa học.

2. Thẩm định về mặt kỹ thuật và công nghệ đối với các dự án, kế hoạch ứng dụng công nghệ thông tin của các cơ quan, đơn vị thuộc và trực thuộc nhà trường.

3. Tiếp nhận và đưa ra các cảnh báo về an toàn, an ninh thông tin, áp dụng các biện pháp để khắc phục và hạn chế tối đa thiệt hại do sự cố mất an toàn, an ninh thông tin trong mạng trường Đại học Khoa học.

4. Kiểm soát các thông tin truyền trong mạng trường Đại học Khoa học. Khi phát hiện ra sự cố mất an toàn, an ninh thông tin, Trung tâm CNTT-TV được phép nhắc nhở, tạm dừng cung cấp các dịch vụ trong mạng trường Đại học Khoa học đối với người sử dụng có liên quan để kiểm tra, khắc phục sự cố. Trường hợp có sự cố nghiêm trọng vượt quá khả năng khắc phục phải báo cáo Ban Giám hiệu và thông báo cho các tổ chức hỗ trợ xử lý sự cố mất an toàn thông tin để cùng phối hợp giải quyết.

5. Bố trí cán bộ, bộ phận chuyên trách về bảo mật, bảo đảm an toàn, an ninh thông tin; xây dựng quy chế, quy trình nội bộ quản lý chức năng đặc quyền; quản lý và bảo đảm an toàn, an ninh thông tin, bảo mật tài khoản, mật khẩu truy cập và các thông tin lưu trữ tại Trung tâm tích hợp dữ liệu của Bộ; thường xuyên thực hiện phân tích, đánh giá, lập báo cáo về mức độ nghiêm trọng của các rủi ro; tổ chức theo dõi và kiểm soát tất cả các phương pháp truy cập từ xa, truy cập trái phép, các nguy cơ dẫn đến làm mất mát, thay đổi hoặc phá hủy thông tin và hệ thống thông tin trong mạng trường Đại học Khoa học.

6. Lựa chọn công nghệ, kỹ thuật hiện đại, xây dựng, triển khai các giải pháp bảo mật, bảo đảm an toàn, an ninh trong mạng trường Đại học Khoa học.

7. Lắp đặt các trang thiết bị, hướng dẫn sử dụng, bảo trì, sao lưu dữ liệu định kỳ, nâng cấp, quản lý và vận hành mạng trường Đại học Khoa học; kiểm tra và xử lý kịp thời các sự cố kỹ thuật, các lỗ hổng bảo mật, bảo đảm hệ thống mạng trường Đại học Khoa học hoạt động ổn định, an toàn và bảo mật.

8. Thường xuyên nghiên cứu, cập nhật cấu hình phần cứng hiện đại, phù hợp với các thành phần của hệ thống thông tin, thiết lập cấu hình chặt chẽ cho các trang thiết bị, phần mềm bảo mật, phần mềm an toàn, an ninh thông tin nhưng vẫn bảo đảm tính tương thích, tính toàn vẹn và tính sẵn sàng của thông tin trong mạng trường Đại học Khoa học.

9. Tổ chức tập huấn, phổ biến kiến thức, kỹ năng về bảo mật, bảo đảm an toàn, an ninh thông tin cho người sử dụng khi được cấp quyền khai thác và sử dụng tài nguyên mạng trường Đại học Khoa học.

10. Lập kế hoạch hàng năm trình Hiệu trưởng trường Đại học Khoa học phê duyệt và tổ chức triển khai kế hoạch phát triển, bảo mật, bảo đảm an toàn, an ninh thông tin trong mạng trường Đại học Khoa học và kế hoạch đào tạo, bồi dưỡng nghiệp vụ cho cán bộ chuyên trách công nghệ thông tin và người sử dụng.

11. Báo cáo Ban Giám hiệu định kỳ (mỗi năm 01 lần vào cuối quý IV) và đột xuất về tình hình và kết quả thực hiện công tác bảo mật, bảo đảm an toàn, an ninh thông tin tại trường Đại học Khoa học.

12. Cấp mới, sửa đổi, thu hồi tài khoản, mật khẩu truy cập và quyền khai thác tài nguyên mạng trường Đại học Khoa học cho người sử dụng khi có yêu cầu.

13. Phối hợp với các đơn vị trong nhà trường xây dựng các quy trình, quy chế, tổ chức tập huấn sử dụng, xây dựng cơ chế kiểm soát và đảm bảo tính bảo mật của các phần mềm được trang bị và phát triển mới.

Điều 8. Trách nhiệm của các cơ quan, đơn vị thuộc và trực thuộc Trường Đại học Khoa học

1. Thủ trưởng các cơ quan, đơn vị thuộc và trực thuộc trường Đại học Khoa học có trách nhiệm quán triệt, chỉ đạo và giám sát cán bộ, công chức, viên chức thuộc đơn vị mình thực hiện đúng Quy chế này.

2. Cung cấp thông tin người sử dụng của đơn vị mình khi có sự thay đổi để Trung tâm CNTT-TV thực hiện cấp mới, sửa đổi, thu hồi tài khoản, mật khẩu truy cập và quyền khai thác tài nguyên mạng trường Đại học Khoa học.

3. Bảo vệ, quản lý các trang thiết bị và tài nguyên mạng trường Đại học Khoa học được lắp đặt tại đơn vị.

4. Chịu trách nhiệm về nội dung, thông tin truyền tải trong mạng trường Đại học Khoa học theo đúng Quy chế này và các quy định hiện hành của pháp luật, của trường Đại học Khoa học.

5. Trường hợp phát hiện sự cố mất an toàn, an ninh thông tin phải thông báo kịp thời tới Trung tâm CNTT-TV bằng văn bản và các hình thức liên lạc khác để phối hợp giải quyết.

6. Tạo điều kiện thuận lợi cho Trung tâm CNTT-TV triển khai công tác kiểm tra, khắc phục sự cố khi xảy ra tình trạng mất an toàn, an ninh thông tin trong mạng trường Đại học Khoa học.

7. Phối hợp với Trung tâm CNTT-TV để lấy ý kiến thẩm định về mặt kỹ thuật và công nghệ đối với các dự án, kế hoạch ứng dụng công nghệ thông tin.

8. Phối hợp với Trung tâm CNTT-TV quy trình, quy chế, tổ chức tập huấn sử dụng, xây dựng cơ chế kiểm soát và đảm bảo tính bảo mật của các phần mềm được trang bị và phát triển mới tại đơn vị.

Điều 9. Trách nhiệm của người sử dụng

1. Nâng cao trách nhiệm bảo mật, bảo đảm an toàn, an ninh thông tin trong mạng trường Đại học Khoa học; thông báo kịp thời tới Trung tâm CNTT-TV trong trường hợp phát hiện ra sự cố mất an toàn, an ninh thông tin.

2. Thực hiện đúng thẩm quyền việc sao chép, chia sẻ, đưa thông tin vào trong mạng trường Đại học Khoa học.

3. Cung cấp thông tin cá nhân chính xác, đầy đủ, giữ bí mật tài khoản cá nhân khi tham gia khai thác, sử dụng mạng trường Đại học Khoa học và hoàn toàn chịu trách nhiệm tất cả các hoạt động của mình trong mạng trường Đại học Khoa học.

4. Không sử dụng mật khẩu mặc định, đơn giản; có trách nhiệm thay đổi mật khẩu định kỳ; khi bị lộ hoặc nghi bị lộ mật khẩu phải thông báo kịp thời tới Trung tâm CNTT-TV phối hợp giải quyết.

5. Thường xuyên kiểm tra và diệt vi rút tin học trên máy tính và các thiết bị lưu trữ dữ liệu cá nhân; phối hợp với Trung tâm CNTT-TV để sử dụng các dịch vụ bảo mật, an toàn, an ninh thông tin; không mở các thư lạ, các tệp tin đính kèm hoặc các đường liên kết, các website không rõ nguồn gốc xuất xứ để tránh bị nhiễm vi rút tin học, các mã độc hại.

6. Không tự ý lắp đặt các trang thiết bị kết nối vào mạng trường Đại học Khoa học, nghiêm cấm việc sử dụng các công cụ, phần mềm làm tổn hại đến hoạt động mạng trường Đại học Khoa học. Không tự ý tắt, hủy cài đặt phần mềm diệt virus đã được nhà trường cài đặt.

7. Tạo điều kiện thuận lợi cho cán bộ chuyên trách khắc phục sự cố mất an toàn, an ninh thông tin. Khi có sự cố kỹ thuật, không được tự ý xử lý mà phải thông báo lại cho TTCNTT-TV.

8. Không sử dụng chung mật khẩu cho nhiều dịch vụ khác nhau trên Internet, nhất là các dịch vụ miễn phí. Không trao đổi, chia sẻ mật khẩu cá nhân, lưu mật khẩu trên các máy tính dùng chung.

9. Không tự ý thay đổi các tham số cài đặt, chiếm quyền điều khiển các thiết bị mạng trường ĐHKH.

10. Không được bao che hoặc dung túng cho kẻ xấu lợi dụng các trang thiết bị, quyền sử dụng tài khoản, mật khẩu để truy cập, phá hoại mạng trường Đại học Khoa học.

11. Tham gia các chương trình đào tạo, hội nghị, hội thảo về bảo mật, bảo đảm an toàn, an ninh thông tin do các đơn vị chuyên trách về công nghệ thông tin tổ chức.

Chương IV

ĐIỀU KHOẢN THI HÀNH

Điều 10. Xử lý vi phạm

Mọi hành vi vi phạm Quy chế này sẽ bị xử lý kỷ luật tùy theo tính chất, mức độ vi phạm khác nhau và theo quy định hiện hành của pháp luật, của Đại học Thái Nguyên và của trường Đại học Khoa học.

Điều 11. Trách nhiệm thi hành

1. Trung tâm CNTT-TV có trách nhiệm hướng dẫn, kiểm tra việc thực hiện Quy chế này; trình Hiệu trưởng để xử lý những trường hợp sai phạm của các cơ quan, đơn vị thuộc và trực thuộc Bộ trong công tác bảo mật, bảo đảm an toàn, an ninh thông tin mạng trường Đại học Khoa học.

2. Thủ trưởng các cơ quan, đơn vị thuộc và trực thuộc Trường vụ trong phạm vi chức năng, nhiệm vụ có trách nhiệm tổ chức triển khai và kiểm tra việc chấp hành tại đơn vị theo đúng các quy định của Quy chế này.

3. Trong quá trình triển khai Quy chế này, nếu có vấn đề phát sinh hoặc vướng mắc, đề nghị các đơn vị phản ánh về trường (qua Trung tâm CNTT-TV) để tổng hợp báo cáo, trình Hiệu trưởng xem xét, quyết định./.

HIỆU TRƯỞNG

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC KHOA HỌC
ĐẠI HỌC THÁI NGUYÊN

PGS.TS. Nông Quốc Chinh