TẬP ĐOÀN DẦU KHÍ VIỆT NAM
TRƯỜNG ĐẠI HỌC DẦU KHÍ VIỆT NAM

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

Số: 295 /QĐ-ĐHDK

Hà Nội, ngày 06 tháng 4 năm 2012

QUYẾT ĐỊNH
Về việc ban hành Quy định quản lý, khai thác và sử dụng hệ thống công nghệ thông tin của Trường Đại học Dầu khí Việt Nam

HIỆU TRƯỞNG
TRƯỜNG ĐẠI HỌC DẦU KHÍ VIỆT NAM

Căn cứ Quyết định số 2157/QĐ-TTg ngày 25/11/2010 của Thủ tướng Chính phủ về việc thành lập Trường Đại học Dầu khí Việt Nam;

Căn cứ Quy chế tổ chức và hoạt động của Trường Đại học Dầu khí Việt Nam ban hành kèm theo Quyết định số 187/QĐ-DKVN ngày 19/01/2011 của Tập đoàn Dầu khí Việt Nam;

Xét đề nghị của Giám đốc Trung tâm Thông tin – Thư viện tại Tờ trình số 13/TTr-TTTV ngày 27/3/2012;

Theo đề nghị của Trưởng phòng Tổ chức – Hành chính,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy định quản lý, khai thác và sử dụng hệ thống công nghệ thông tin của Trường Đại học Dầu khí Việt Nam.

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

Điều 3. Trưởng phòng Tổ chức – Hành chính, Giám đốc Trung tâm Thông tin – Thư viện và CBNV chịu trách nhiệm thi hành Quyết định này.

Nơi nhận:
- Như điều 3;
- HĐT (để b/e);
- Ban giám hiệu (e-copy);
- Trưởng các đơn vị (e-copy);
- Lưu: VT, TCHC

HIỆU TRƯỞNG

TRƯỜNG ĐẠI HỌC DẦU KHÍ VIỆT NAM

Lê Phước Hảo

TẬP ĐOÀN DẦU KHÍ VIỆT NAM
TRƯỜNG ĐẠI HỌC DẦU KHÍ VIỆT NAM

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

QUY ĐỊNH QUẢN LÝ, KHAI THÁC VÀ SỬ DỤNG HỆ THỐNG CÔNG NGHỆ THÔNG TIN CỦA TRƯỜNG ĐẠI HỌC DẦU KHÍ VIỆT NAM

(Ban hành kèm theo Quyết định số 295 /QĐ-ĐHDK ngày 06 tháng 4 năm 2012 của Hiệu trưởng Trường Đại học Dầu khí Việt Nam)

Chương I

NHỮNG QUY ĐỊNH CHUNG

Điều 1. Phạm vi và đối tượng áp dụng

1. Quy định này quy định về việc sử dụng hệ thống công nghệ thông tin (CNTT) của Trường Đại học Dầu khí Việt Nam (PVU) gồm:

- Quản lý, khai thác mạng máy tính của PVU.
- Sử dụng hệ thống máy chủ.
- Sử dụng hệ thống Email.
- Các quy định về đảm bảo an toàn, an ninh thông tin và bảo mật trên môi trường mạng trong hoạt động của PVU.

2. Quy định này được áp dụng đối với các đơn vị, cá nhân sử dụng hệ thống CNTT của PVU.

Điều 2. Các thuật ngữ

1. Hệ thống CNTT: Hệ thống CNTT của PVU bao gồm hệ thống các máy tính, thiết bị tin học, hệ thống đường truyền, mạng LAN và các ứng dụng, cơ sở dữ liệu (CSDL) chạy trên hệ thống mạng này.

2. Mạng cục bộ (LAN): bao gồm các máy chủ, máy trạm, thiết bị mạng, đường truyền và các thiết bị ngoại vi được liên kết với nhau.

3. Mạng máy tính của PVU (sau đây gọi là mạng PVU): là hệ thống mạng diện rộng (WAN) kết nối các mạng LAN tại các cơ sở đào tạo của PVU; bao gồm các thiết bị ngoại vi và các thiết bị truyền nhận thông tin.

4. Hệ thống máy chủ: Gồm các máy chủ lưu trữ quản lý thông tin, dữ liệu kết hợp với hệ thống đường truyền nhằm trao đổi thông tin, dữ liệu trên môi trường mạng LAN, WAN và Internet. Hệ thống này bao gồm các dịch vụ lưu trữ CSDL,Web, truyền nhận và lưu trữ dữ liệu…

5. Hệ thống thư điện tử (Email): là hệ thống quản lý và cung cấp dịch vụ thư điện tử của PVU với tên miền "pvu.edu.vn".

6. An toàn thông tin: Bao gồm các hoạt động quản lý, nghiệp vụ và kỹ thuật đối với hệ thống thông tin, nhằm bảo vệ, khôi phục các hệ thống, các dịch vụ và nội dung thông tin đối với các nguy cơ chủ quan hoặc khách quan. Việc bảo vệ thông tin, tài sản và con người trong hệ thống thông tin nhằm bảo đảm cho các hệ thống thực hiện đúng chức năng, phục vụ đúng đối tượng một cách sẵn sàng, chính xác và tin cậy. An toàn thông tin bao hàm các nội dung bảo vệ và bảo mật thông tin, an toàn dữ liệu, an toàn máy tính và an toàn mạng.

7. Tài sản CNTT: là các trang thiết bị, thông tin thuộc hệ thống CNTT, bao gồm:

a) *Tài sản vật lý:* là các thiết bị CNTT, phương tiện truyền thông và các thiết bị phục vụ cho hoạt động của hệ thống CNTT.

b) *Tài sản thông tin:* là các dữ liệu, tài liệu liên quan đến hệ thống CNTT. Tài sản thông tin được thể hiện bằng văn bản giấy hoặc dữ liệu điện tử.

c) *Tài sản phần mềm:* bao gồm các chương trình ứng dụng, phần mềm hệ thống, cơ sở dữ liệu và công cụ phát triển.

8. Tường lửa (Firewall): là tập hợp các thành phần hoặc một hệ thống các trang thiết bị, phần mềm được đặt giữa hai mạng, nhằm kiểm soát tất cả các kết nối từ bên trong ra bên ngoài mạng hoặc ngược lại.

9. Virus: là chương trình máy tính có khả năng lây lan, gây ra hoạt động không bình thường cho thiết bị số hoặc sao chép, sửa đổi, xóa bỏ thông tin lưu trữ trong thiết bị số.

10. Phần mềm độc hại (mã độc): là các phần mềm có tính năng gây hại như virus, phần mềm do thám (spyware), phần mềm quảng cáo (adware) hoặc các dạng tương tự khác.

Chương II

QUẢN LÝ, KHAI THÁC MẠNG MÁY TÍNH CỦA PVU

Điều 3. Đơn vị quản lý mạng PVU

1. Trung tâm Thông tin – Thư viện (sau đây gọi tắt là Trung tâm) là đơn vị được PVU giao quản lý mạng PVU, có trách nhiệm định kỳ hàng năm báo cáo bằng văn bản với Ban Giám hiệu về tình hình hoạt động của mạng và các vấn đề phát sinh.

2. Các đơn vị và cá nhân thuộc PVU có trách nhiệm khai thác, bảo vệ mạng của đơn vị và mạng PVU.

Điều 4. Các hoạt động quản lý mạng PVU

1. Nội dung công tác quản lý mạng PVU bao gồm: quản lý các máy chủ, máy trạm, thiết bị mạng, hệ thống cáp mạng, thông số kỹ thuật mạng; bảo đảm hoạt động của các máy tính trên hệ thống mạng, bảo mật và an toàn thông tin; giải quyết các sự cố liên quan.

2. Quản trị và duy trì hoạt động của mạng PVU đảm bảo các dịch vụ chia sẻ dữ liệu, Email, Web, CSDL và Internet hoạt động tốt; đảm bảo các hoạt động hỗ trợ kỹ thuật cho các đơn vị trong PVU vào các ngày làm việc; phối hợp với các đơn vị trong

PVU để đảm bảo cho hệ thống mạng hoạt động tốt.

3. Cung cấp các dịch vụ mạng máy tính tin cậy và hiệu quả cho các đơn vị và cá nhân trong PVU. Thực hiện các hoạt động duy trì, sửa chữa và nâng cấp cho mạng PVU như xử lý các yêu cầu về di chuyển, các thay đổi thông số hệ thống mạng, tạo và thay đổi tài khoản sử dụng mạng…

4. Trường hợp tạm ngừng cung cấp dịch vụ mạng để sửa chữa, nâng cấp, cập nhật phải thông báo trước cho đơn vị, cá nhân sử dụng mạng biết trước tối thiểu 1 ngày.

5. Kiểm tra, giám sát việc sử dụng các kết nối và các dịch vụ mạng PVU đã cấp cho các đơn vị, cá nhân tham gia vào mạng; được quyền yêu cầu các đơn vị tham gia vào mạng của PVU phải cung cấp các thông tin và các số liệu liên quan tới mạng của đơn vị.

6. Trong trường hợp các đơn vị, cá nhân không tuân thủ các điều kiện đảm bảo kỹ thuật của mạng sẽ bị tạm dừng cung cấp dịch vụ sau khi đã được nhắc nhở.

Điều 5. Khai thác sử dụng mạng PVU

1. Các đơn vị và cá nhân trong PVU đều được quyền đăng ký sử dụng các dịch vụ mạng hiện có và có trách nhiệm bảo đảm an toàn, an ninh cho hệ thống thiết bị và thông tin của mình trên mạng PVU.

2. Các đơn vị trong PVU khi có nhu cầu xây dựng, sửa chữa, hay đăng ký kết nối mạng với các tổ chức khác để truy cập cơ sở dữ liệu phải báo cho Trung tâm biết trước 03 ngày để giám sát việc thực hiện và đảm bảo phù hợp quy hoạch tổng thể mạng PVU.

3. Các đơn vị và cá nhân trong PVU khi sử dụng các dịch vụ mạng phải chịu trách nhiệm khai thác các dịch vụ mạng đúng mục đích, đúng yêu cầu trong phạm vi cho phép.

Điều 6. Nguyên tắc cung cấp và sử dụng dịch vụ mạng

1. Các dịch vụ mạng được cung cấp bao gồm: email, lưu trữ CSDL,Web, truyền nhận và lưu trữ dữ liệu…được PVU cho phép sử dụng và các dịch vụ mạng khác phục vụ cho công tác đào tạo, quản lý của PVU và đơn vị.

2. Các đơn vị và cá nhân thuộc PVU khi tham gia vào mạng máy tính không được tự ý thay đổi những thông số liên quan đến mạng PVU. Trường hợp cần thay đổi phải được sự đồng ý bằng văn bản của Trung tâm.

Điều 7. Kết nối mạng PVU

1. Tất cả các đơn vị, cá nhân trong PVU có nhu cầu thiết lập kết nối mạng PVU, tài khoản sử dụng dịch vụ mạng PVU phải đăng ký bằng văn bản với Trung tâm. Thời gian đăng ký vào giờ làm việc tất cả các ngày trong tuần (từ thứ Hai đến thứ Sáu). Thời gian thực hiện cung cấp dịch vụ mạng PVU cho các máy tính là trong vòng 2 ngày tùy theo từng dịch vụ kể từ khi Trung tâm nhận được bản đăng ký.

2. Trung tâm có quyền từ chối cung cấp dịch vụ mạng cho các máy tính có kết

nối mạng không tuân thủ theo Quy định này.

Điều 8. Bảo đảm an toàn thông tin, dữ liệu

Trung tâm chịu trách nhiệm đảm bảo an toàn thông tin truyền dẫn và dữ liệu lưu chuyển trên mạng PVU, áp dụng các biện pháp đảm bảo an ninh, bảo mật những thông tin trên mạng PVU, bảo quản sao lưu dữ liệu được thực hiện trên các máy chủ đặt tại Trung tâm.

Chương III

HỆ THỐNG MÁY CHỦ

Điều 9. Quy định chung của hệ thống máy chủ

1. Hệ thống máy chủ cho phép lưu trữ và quản lý dữ liệu trên máy chủ và thực hiện các dịch vụ trên LAN, WAN, Internet..., nhằm phục vụ công tác quản lý, điều hành của các đơn vị sử dụng dịch vụ.

2. Hệ thống máy chủ được áp dụng cho tất cả các đơn vị có nhu cầu tham gia khai thác, sử dụng hệ thống mạng PVU.

Điều 10. Tổ chức quản lý và vận hành hệ thống máy chủ

a) Trách nhiệm của đơn vị/cá nhân sử dụng dịch vụ máy chủ

1. Việc quản lý và đưa thông tin lên Website của đơn vị và của PVU phải tuân thủ theo các quy định của Bộ Văn hoá - Thể thao và Du lịch và của PVU.

2. Không được làm phương tiện để truyền nhận các thông tin xấu, phản động chống lại Nhà nước Việt Nam.

3. Phải tự chịu trách nhiệm và đảm bảo việc sử dụng nội dung dữ liệu trên máy chủ vào những mục đích hợp pháp, đặc biệt không sử dụng cho những trường hợp sau:

- Dùng dịch vụ máy chủ trong các ứng dụng vi phạm bản quyền phần mềm, sở hữu trí tuệ,... đồng thời có trách nhiệm kiểm soát và ngăn cấm người khác làm điều đó.
- Gửi, tạo liên kết hoặc trung chuyển bất kỳ loại dữ liệu nào mang tính bất hợp pháp, đe dọa, lừa dối, thù hằn, xuyên tạc, nói xấu, tục tĩu, khiêu dâm, xúc phạm...hay các hình thức bị ngăn cấm khác dưới bất kỳ cách thức nào.
- Thực hiện các hình thức spam email mang mục đích phá hoại từ máy chủ hay hệ thống mạng.
- Các chương trình có khả năng làm tắc nghẽn hoặc đình trệ hệ thống, như gây cạn kiệt tài nguyên hệ thống, làm quá tải bộ vi xử lý và bộ nhớ.
- Cài đặt các chương trình chat (tán gẫu), các file nhạc (mp3, ram, wma,...), Video (.avi .dat .mp4), các tài liệu số và các phần mềm không có bản quyền.

4. Có trách nhiệm bảo mật các thông tin như mật khẩu hay những thông tin mật khác liên quan đến tài khoản của đơn vị và có trách nhiệm thông báo cho đơn vị quản lý hệ thống máy chủ khi phát hiện các hình thức truy cập trái phép bằng tài khoản hoặc các sơ hở về bảo mật, bao gồm việc mất mát, đánh cắp hoặc để lộ các thông tin về mật

khẩu và các thông tin liên quan khác.

5. Tuân thủ các yêu cầu kỹ thuật quy định của hệ thống trong quy định này và không được dùng máy chủ vào những mục đích có thể gây ảnh hưởng đến hoạt động hệ thống và có trách nhiệm tự sao lưu bảo quản dữ liệu của mình.

6. Nếu vi phạm các qui định nêu trên, hệ thống sẽ ngừng cung cấp dịch vụ mà không thông báo trước để đảm bảo an toàn cho hệ thống.

b) Trách nhiệm của Trung tâm

1. Hệ thống máy chủ do các cán bộ kỹ thuật của Trung tâm quản lý và vận hành bảo đảm cho Hệ thống hoạt động thông suốt, liên tục.

2. Bảo đảm an toàn, bảo mật thông tin theo chế độ mật; quản lý quyền truy cập của đơn vị sử dụng dịch vụ.

3. Đảm bảo hệ thống được phòng chống virus, spam… và bảo quản dữ liệu của đơn vị sử dụng dịch vụ trên hệ thống.

4. Đơn vị sử dụng dịch vụ sẽ được thông báo ngay trong vòng 12 giờ khi có sự cố đáng tiếc xảy ra như hỏng thiết bị phần cứng, đường truyền truy cập bị lỗi, lỗi DNS của dịch vụ.... Các sự cố bất khả kháng xảy ra với hệ thống sẽ được khắc phục trong thời gian sớm nhất.

5. Có quyền loại bỏ tài khoản, cắt dịch vụ khi đơn vị sử dụng vi phạm các điều trong mục a).

Chương IV

HỆ THỐNG THƯ ĐIỆN TỬ (EMAIL)

Điều 11. Quy định chung đối với hệ thống thư điện tử

1. Hệ thống thư điện tử của PVU được sử dụng để gửi, nhận thông tin dưới dạng thư điện tử qua mạng tin học của PVU phục vụ công tác quản lý điều hành và chuyên môn, nghiệp vụ theo chức năng được phân công.

2. Cá nhân thuộc PVU bắt buộc phải sử dụng hộp thư có tên miền "pvu.edu.vn" trong trao đổi thông tin điện tử phục vụ cho công tác. Thành viên BGH và một số lãnh đạo các đơn vị được sử dụng email của Trường và của PVN để liên hệ công tác, trong trường hợp này cá nhân phải đảm bảo sử dụng hiệu quả.

3. Các loại hộp thư điện tử:

- Hộp thư cá nhân: là các hộp thư dành cho cá nhân của PVU.
- Hộp thư đơn vị: là các hộp thư sử dụng chung của các đơn vị thuộc PVU.

4. Danh bạ thư điện tử: lưu trữ thông tin về tổ chức, cá nhân sử dụng hộp thư điện tử như tên đơn vị/cá nhân, địa chỉ, email, ngày đăng ký sử dụng.

Điều 12. Cách đặt tên cho các hộp thư của PVU

1. Hộp thư cá nhân đặt tên như sau: <tên người sử dụng>><ký tự đầu của họ và tên đệm>@pvu.edu.vn. Trong trường hợp trùng tên thì tuân thủ theo quy tắc sau: <tên

cán bộ><ký tự đầu của họ và tên đệm><số thứ tự>@pvu.edu.vn..

2. Hộp thư chung của đơn vị đặt tên như sau: <tên đơn vị>@pvu.eduvn. Trong đó <tên đơn vị> là ký hiệu tắt của đơn vị sao cho dễ phân biệt.

Điều 13. Trách nhiệm của đơn vị và cá nhân sử dụng thư điện tử

1. Các đơn vị gửi danh sách cán bộ đăng ký sử dụng hoặc thôi sử dụng hộp thư điện tử của PVU cho Trung tâm để khởi tạo hộp thư mới hoặc xoá bỏ hộp thư không sử dụng nữa. Mỗi cá nhân chỉ được phép sử dụng một hộp thư điện tử duy nhất của PVU.

2. Các đơn vị cung cấp các thông tin thay đổi về nhân sự, tổ chức của đơn vị cho Trung tâm để kịp thời điều chỉnh hộp thư cho phù hợp.

3. Các cá nhân, đơn vị không tự động tổ chức hệ thống thư điện tử riêng và không sử dụng hộp thư cá nhân công cộng (như Hotmail, Yahoo, Gmail,...) vào mục đích giao dịch công việc của PVU.

4. Cá nhân sử dụng hộp thư điện tử có trách nhiệm quản lý nội dung thư và bảo vệ mật khẩu thư điện tử của mình, chịu trách nhiệm trước pháp luật về nội dung trao đổi qua thư điện tử.

5. Mỗi cá nhân được phép sử dụng 25GB để lưu trữ email trên máy chủ thư điện tử. Khi có nhiều thông tin cá nhân vượt quá dung lượng lưu trữ phải chuyển thông tin về máy của mình bằng các phần mềm sử dụng email.

6. Cá nhân sử dụng hộp thư không tự ý truy cập vào hộp thư của người khác hoặc để người khác sử dụng hộp thư điện tử của mình, không phát tán thư rác, khi gặp sự cố về hệ thống thư điện tử phải thông báo cho Trung tâm biết để khắc phục.

7. Các cá nhân đang sử dụng hộp thư điện tử của PVU mà chuyển cơ quan khác hoặc nghỉ việc, nghỉ hưu,.. thì đơn vị có trách nhiệm thông báo cho Trung tâm biết để chuyển hoặc xoá tên khỏi danh sách hộp thư điện tử. Nếu đơn vị không thông báo thì thủ trưởng đơn vị phải chịu trách nhiệm trước PVU về việc sử dụng thư điện tử không đúng mục đích.

8. Hộp thư của đơn vị do thủ trưởng đơn vị quản lý, thủ trưởng có thể uỷ quyền cho một hoặc một số người trong đơn vị sử dụng.

9. Khi thay đổi thủ trưởng đơn vị thì thủ trưởng cũ phải bàn giao hộp thư và mật khẩu và nội dung dữ liệu của đơn vị cho thủ trưởng mới.

Điều 14. Trách nhiệm của Trung tâm trong quản lý hệ thống thư điện tử của PVU

1. Quản lý, vận hành đảm bảo kỹ thuật và cung cấp các dịch vụ cơ bản cho hệ thống thư điện tử của PVU hoạt động thông suốt, liên tục.

2. Bảo đảm an toàn, bảo mật thông tin hộp thư cá nhân, quản lý quyền truy cập cho hệ thống thư điện tử.

3. Cài đặt hệ thống phòng chống virus, spam và ngăn chặn thư rác có nội dung không phù hợp với công tác chuyên môn, nghiệp vụ.

4. Tạo lập chế độ lưu trữ thông tin, cung cấp, thay đổi hoặc huỷ bỏ hộp thư điện tử cho cán bộ công chức theo đề nghị của các đơn vị thuộc cơ cấu tổ chức của PVU.

5. Đối với cán bộ chuyển đổi công tác, nghỉ hưu,...Trung tâm căn cứ vào đề nghị của đơn vị để cập nhật thông tin mới hoặc xoá hộp thư của cá nhân hoặc đơn vị này.

6. Thông tin cho các đơn vị biết về hộp thư điện tử của PVU. Định kỳ báo cáo tình hình sử dụng email cho lãnh đạo.

7. Tổ chức đào tạo hướng dẫn sử dụng, khai thác hệ thống thư điện tử có hiệu quả.

Chương V

NỘI DUNG ĐẢM BẢO AN TOÀN, AN NINH HỆ THỐNG THÔNG TIN

Điều 15. Mục đích đảm bảo an toàn, an ninh thông tin và bảo mật trên môi trường mạng

1. Giảm thiểu các nguy cơ gây sự cố mất an toàn thông tin và đảm bảo an ninh thông tin trong quá trình tham gia hoạt động trên mạng Internet.

2. Công tác đảm bảo an ninh thông tin, bảo mật trên môi trường mạng là một trong những nhiệm vụ trọng tâm để đảm bảo an toàn về cơ sở dữ liệu, các thiết bị trong việc ứng dụng CNTT trong quản lý.

Điều 16. An toàn, bảo mật tài sản CNTT

1. Tài sản CNTT phải được bố trí, lắp đặt tại các địa điểm an toàn và được bảo vệ để giảm thiểu những rủi ro do các đe dọa, hiểm họa từ môi trường và các xâm nhập trái phép.

2. Tài sản CNTT phải được bảo đảm về nguồn điện và các hệ thống hỗ trợ khi nguồn điện chính bị gián đoạn. Phải có biện pháp chống quá tải hay sụt giảm điện áp, chống sét lan truyền; có hệ thống máy phát điện dự phòng và hệ thống lưu điện đảm bảo thiết bị hoạt động liên tục.

3. Hệ thống máy chủ được đặt cố định trong phòng riêng và được bảo vệ an toàn; nguồn điện cung cấp cho hệ thống máy chủ phải ổn định; có điều hòa nhiệt độ để đảm bảo về nhiệt độ và độ ẩm phù hợp với yêu cầu tiêu chuẩn kỹ thuật phòng máy.

4. Tất cả các thiết bị lưu trữ dữ liệu phải được kiểm tra để đảm bảo các dữ liệu quan trọng và phần mềm có bản quyền lưu trữ trên thiết bị được xóa bỏ hoặc ghi đè không có khả năng khôi phục trước khi loại bỏ hoặc tái sử dụng cho mục đích khác.

5. Những máy tính có chứa dữ liệu quan trọng cần được bảo vệ và thường xuyên có kết nối Internet phải cài đặt phần mềm diệt virus tin cậy, có bản quyền trên những máy tính đó; cấu hình hệ thống mạng máy tính nội bộ của cơ quan, đơn vị kết nối với mạng Internet qua thiết bị Firewall;

6. Tài sản CNTT chỉ được đưa ra bên ngoài đơn vị khi có sự cho phép của cấp

có thẩm quyền.

7. Các trang thiết bị dùng cho hoạt động nghiệp vụ lắp đặt bên ngoài trụ sở của đơn vị phải có biện pháp giám sát, bảo vệ an toàn phòng chống truy cập bất hợp pháp.

Điều 17. Bảo đảm an toàn thông tin, dữ liệu

1. Đối với phần mềm

a) Phần mềm đã được cơ quan, đơn vị mua bản quyền nhằm phục vụ cho việc đảm bảo an toàn cho hệ thống thông tin yêu cầu tất cả các cán bộ, viên chức sử dụng máy tính phải cài đặt và thường xuyên cập nhật phiên bản mới theo hướng dẫn của nhà cung cấp;

b) Các phần mềm ứng dụng như: Phần mềm kế toán, quản lý nhân sự, tiền lương, đào tạo, thư viện, phần mềm báo cáo số liệu... phải đảm bảo tính chính xác của thông tin, không gây ra sự cố mất dữ liệu, đảm bảo hệ thống phần mềm luôn hoạt động liên tục.

2. Đối với dữ liệu

a) Định kỳ ít nhất 1 tháng một lần, đơn vị phải tiến hành tổ chức lưu trữ, sao chép dữ liệu ra bộ nhớ ngoài như: ổ cứng gắn ngoài, đĩa CD, USB... (dữ liệu trong các máy tính phải tiến hành sao chép để bảo vệ là những dữ liệu chuyên môn phục vụ công tác của cơ quan, đơn vị);

b) Các thiết bị lưu trữ thông tin này phải được bảo quản ở nơi an toàn và bảo mật. Các dữ liệu có tính chất quan trọng cần phải được mã hóa nhằm bảo vệ khỏi bị đánh cắp, lộ thông tin.

2. Đối với máy tính, thiết bị tháo lắp (USB, máy tính xách tay)

a) Đơn vị, cá nhân thuộc trường được giao sử dụng máy tính phải đặt mật khẩu truy cập vào máy tính của mình;

b) Sử dụng thiết bị lưu trữ (USB) an toàn, đúng cách để phòng ngừa virus xâm nhập máy tính: Khi trao đổi dữ liệu giữa USB và máy tính, không được trực tiếp truy nhập ngay vào USB vì có thể rất nhiều virus được kích hoạt và lây lan vào máy tính thông qua thao tác đó; phải quét virus đối với USB bằng phần mềm diệt virus, sau đó mới được truy cập bình thường;

c) Khi phát hiện các nguy cơ mất an toàn hoặc sự cố phải báo ngay cho cán bộ quản trị mạng để ngăn chặn, xử lý kịp thời.

3. Truyền tải, lưu trữ, sao chép thông tin

a) Để đảm bảo an toàn thông tin, mọi cá nhân đã được cấp địa chỉ email trong Hộp thư điện tử của Trường cần đổi mật khẩu ban đầu; sử dụng Hệ thống thư điện tử để truy nhập, thu thập, chia sẻ dữ liệu, truyền tải thông tin, tài liệu... trên môi trường mạng;

b) Không được lưu trữ dữ liệu và sao chép thông tin trên đĩa cứng C, việc lưu trữ dữ liệu và sao chép thông tin chỉ thực hiện trên đĩa cứng D, E hoặc trên USB, giúp cho việc phục hồi mọi dữ liệu trên đĩa C được dễ dàng hơn khi có sự cố máy tính xảy ra.

Điều 18. Trách nhiệm của đơn vị và cá nhân thuộc Trường

1. Có trách nhiệm quản lý, bảo quản thiết bị được giao sử dụng; không tự ý thay đổi cấu hình hoặc tháo lắp các thiết bị trên máy tính khi chưa có sự đồng ý của đơn vị chức năng;

2. Không truy cập thông tin hoặc nhấp chuột vào trang web có đường dẫn lạ không rõ về nội dung (các phần mềm gián điệp được gửi đi với mục đích đánh cắp thông tin mật của người dùng máy tính...); không tải và cài đặt các phần mềm chưa rõ nguồn gốc, không liên quan đến công việc chuyên môn. Không mở các thư điện tử lạ, các tệp tin đính kèm hoặc các liên kết trong các thư lạ để tránh vi rút, mã độc. Hạn chế tải những file có dung lượng lớn (trên 300 MB) trong giờ làm việc, sẽ làm ảnh hưởng đến tốc độ đường truyền của hệ thống;

3. Tuân thủ các biện pháp phòng, chống virus tin học. Mọi dữ liệu từ các thiết bị lưu trữ cầm tay phải được quét diệt virus trước khi sử dụng. Những máy tính phát hiện bị virus tấn công phải được ngắt khỏi mạng PVU để tránh tình trạng lây nhiễm sang các máy tính khác. Báo ngay cho cán bộ Trung tâm xử lý trong trường hợp phát hiện nhưng không diệt được vi rút, mã độc.

4. Nghiêm chỉnh chấp hành các quy định nội bộ về an toàn thông tin của PVU 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; Nghiêm cấm phát tán các thông tin chưa được công bố của Nhà trường khi chưa có sự đồng ý của Hiệu trưởng dưới mọi hình thức.

5. Tham gia các chương trình đào tạo, hội nghị về an toàn, an ninh thông tin do cơ quan cấp trên tổ chức.

Điều 19. Trách nhiệm của Trung tâm

1. Quản lý, vận hành hoạt động của toàn bộ hệ thống mạng máy tính của PVU theo nhiệm vụ được phân công. Tham mưu cho Ban Giám hiệu trong việc đầu tư thiết bị phần cứng, phần mềm, công tác bảo mật thông tin trên môi trường mạng; sử dụng phần mềm có bản quyền và phần mềm mã nguồn mở cho hệ thống máy tính; cập nhật cấu hình chuẩn cho các thành phần của hệ thống khi tiến hành cài đặt và thiết lập cấu hình chặt chẽ nhất cho các sản phẩm an toàn thông tin nhưng vẫn duy trì yêu cầu hoạt động của hệ thống thông tin của PVU;

2. Tổ chức quản lý tài khoản, phân quyền người sử dụng theo nhóm. Hủy ngay quyền truy cập hệ thống thông tin đối với cá nhân nghỉ chế độ, chuyển công tác;

3. Sao chép, lưu trữ thông tin tại nơi an toàn; kiểm tra thông tin sao lưu để đảm bảo tính sẵn sàng và toàn vẹn của thông tin. Xử lý các sự cố về an toàn, an ninh thông tin và bảo mật hệ thống thông tin; định kỳ quét virus tin học cho các máy chủ và hướng dẫn cài đặt, cách phòng, chống virus tin học cho các đơn vị và cá nhân thuộc PVU.

4. Triển khai các biện pháp chống virus, thư rác cho hệ thống máy chủ và tại các máy trạm, các thiết bị di động trong mạng của cơ quan. Sử dụng biện pháp chống virus, thư rác để phát hiện và loại trừ những đoạn mã độc hại (virus, trojan...) được truyền tải bởi: thư điện tử, tập tin đính kèm từ Internet, thiết bị lưu trữ tháo lắp để khai

thác lỗ hổng của hệ thống thông tin. Thường xuyên cập nhật các phần mềm chống virus, thư rác... phù hợp với quy trình quản lý cấu hình hệ thống thông tin của cơ quan, đơn vị;

5. Thực hiện việc đánh giá, báo cáo và đề xuất với Ban Giám hiệu các biện pháp phòng chống các rủi ro và mức độ nghiêm trọng của rủi ro đối với hệ thống thông tin của cơ quan, đơn vị (các rủi ro có thể xảy ra do truy cập, sử dụng thông tin trái phép; mất thông tin; thay đổi hoặc phá hủy thông tin của hệ thống).

Chương VI

ĐIỀU KHOẢN THI HÀNH

Điều 20. Trách nhiệm thi hành

Các đơn vị, cá nhân thuộc PVU chịu trách nhiệm thi hành Quy định này.

Thủ trưởng các đơn vị thuộc PVU có trách nhiệm quán triệt, chỉ đạo và giám sát cá nhân thuộc đơn vị mình thực hiện đúng nội dung Quy định này.

Điều 21. Xử lý vi phạm

1. Các đơn vị và cá nhân thuộc PVU sử dụng hệ thống CNTT của PVU phải tuyệt đối tuân thủ theo Quy định này và phải có trách nhiệm bảo vệ hệ thống CNTT. Mọi hoạt động vi phạm Quy định sẽ bị xử lý kỷ luật tuỳ theo tính chất, mức độ vi phạm khác nhau và theo quy định của pháp luật hiện hành; Nếu vi phạm gây thiệt hại đến tài sản, thiết bị, thông tin, dữ liệu trên mạng máy tính thì cá nhân vi phạm còn phải chịu trách nhiệm bồi thường theo quy định của pháp luật.

2. Các đơn vị sử dụng hệ thống CNTT có hiện tượng vi phạm Quy định đã được nhắc nhở, thông báo mà vẫn tiếp tục vi phạm sẽ được báo cáo lên Ban Giám hiệu để xem xét kỷ luật.

Điều 22. Tổ chức thực hiện

Quy định này có hiệu lực từ ngày ký. Trong quá trình triển khai, nếu có vướng mắc, các đơn vị cần phản ánh kịp thời về Trung tâm xem xét và trình Hiệu trưởng bổ sung, sửa đổi Quy định cho phù hợp./.

HIỆU TRƯỞNG

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC DẦU KHÍ VIỆT NAM
PVU

PGS. TS. Lê Phước Hảo