BỘ KẾ HOẠCH VÀ ĐẦU TƯ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 1180 /QĐ-BKHĐT	*Hà Nội, ngày 24 tháng 8 năm 2015*

QUYẾT ĐỊNH

Ban hành Quy chế đảm bảo an toàn, an ninh thông tin trên mạng máy tính Bộ Kế hoạch và Đầu tư

BỘ TRƯỞNG BỘ KẾ HOẠCH VÀ ĐẦU TƯ

Căn cứ Luật Công nghệ thông tin số 67/2006/QH11 ngày 29/6/2006;

Căn cứ Pháp lệnh bảo vệ bí mật Nhà nước ngày 28/12/2000;

Căn cứ Nghị định số 33/2002/NĐ-CP ngày 28/3/2002 của Chính phủ quy định chi tiết thi hành Pháp lệnh bảo vệ bí mật nhà nước;

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 116/2008/NĐ-CP ngày 14/11/2008 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Kế hoạch và Đầu tư;

Căn cứ Chỉ thị số 879/CT-TTg ngày 10/6/2011 của Thủ tướng Chính phủ về việc tăng cường triển khai các hoạt động đảm bảo an toàn thông tin số;

Căn cứ Chỉ thị số 15/CT-TTg ngày 17/6/2014 của Thủ tướng Chính phủ về tăng cường công tác bảo đảm an ninh và an toàn thông tin mạng trong tình hình mới;

Xét đề nghị của Giám đốc Trung tâm Tin học,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế đảm bảo an toàn, an ninh thông tin trên mạng máy tính Bộ Kế hoạch và Đầu tư.

Điều 2. Quyết định này có hiệu lực kể từ ngày ký, thay thế Quyết định số 1108/QĐ-BKH ngày 27/8/2008 của Bộ trưởng về việc ban hành Quy chế bảo đảm an toàn, an ninh mạng máy tính và thông tin trên mạng tại Bộ Kế hoạch và Đầu tư.

Điều 3. Chánh Văn phòng Bộ, Giám đốc Trung tâm Tin học, Thủ trưởng các đơn vị thuộc Bộ chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Lãnh đạo Bộ;
- Đảng ủy, Công đoàn cơ quan;
- Các đơn vị thuộc Bộ;
- Lưu: VT, TTTH (03 bản).T85

BỘ TRƯỞNG

Bùi Quang Vinh

BỘ KẾ HOẠCH VÀ ĐẦU TƯ

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

QUY CHẾ
Đảm bảo an toàn, an ninh thông tin trên mạng máy tính Bộ Kế hoạch và Đầu tư

(Ban hành kèm theo Quyết định số 1180/QĐ-BKHĐT ngày 24 tháng 8 năm 2015 của Bộ trưởng Bộ Kế hoạch và Đầu tư)

Chương I
QUY ĐỊNH CHUNG

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

1. Quy chế này quy định về công tác đảm bảo an toàn, an ninh thông tin trên mạng máy tính Bộ Kế hoạch và Đầu tư.

2. Quy chế này được áp dụng với các đơn vị, tổ chức, cá nhân liên quan đến việc ứng dụng công nghệ thông tin của Bộ Kế hoạch và Đầu tư.

Điều 2. Giải thích từ ngữ

1. "Mật khẩu an toàn" là mật khẩu đáp ứng yêu cầu sau: Có tối thiểu 8 ký tự. Trong đó có tối thiểu 3 trong số 4 loại ký tự sau: chữ cái viết hoa (A-Z), chữ cái viết thường (a-z), chữ số (0-9), các ký tự khác trên bàn phím máy tính (~, !, ...).

2. "WPA2-Enterprise" là kiểu xác thực sử dụng tên đăng nhập và mật khẩu.

Điều 3. Mục đích, nguyên tắc chung

1. Việc áp dụng Quy chế này nhằm giảm thiểu được các nguy cơ gây mất an toàn thông tin và đảm bảo an ninh thông tin trong quá trình ứng dụng công nghệ thông tin trong hoạt động của các đơn vị, tổ chức, cá nhân liên quan đến việc ứng dụng công nghệ thông tin của Bộ Kế hoạch và Đầu tư.

2. Các hoạt động ứng dụng công nghệ thông tin phải tuân theo nguyên tắc đảm bảo an toàn thông tin được quy định tại Điều 41, Nghị định 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước và các quy định khác của pháp luật về an toàn, an ninh thông tin.

Chương II
QUY ĐỊNH VỀ AN TOÀN, AN NINH THÔNG TIN

Điều 4. Quản lý Trung tâm dữ liệu

1. Trung tâm dữ liệu là khu vực hạn chế tiếp cận và được lắp đặt hệ thống camera giám sát cả bên trong và bên ngoài. Chỉ những người có trách nhiệm

theo quy định của Bộ hoặc của đơn vị quản lý vận hành mới được phép vào Trung tâm dữ liệu.

2. Toàn bộ thiết bị trong Trung tâm dữ liệu phải được lắp đặt, cài đặt, cấu hình đúng tiêu chuẩn kỹ thuật chung của Trung tâm dữ liệu. Tủ thiết bị trong Trung tâm dữ liệu phải được khóa trừ thời gian thực hiện công việc.

3. Quản lý việc mang thiết bị vào, ra Trung tâm dữ liệu

a) Việc mang thiết bị vào, ra để lắp đặt hoặc sửa chữa phải có sự đồng ý của Lãnh đạo đơn vị quản lý, vận hành.

b) Thời gian tháo, lắp thiết bị: thực hiện ngoài giờ hành chính trừ trường hợp xử lý sự cố khẩn cấp; Trước khi mang vào Trung tâm dữ liệu thiết bị phải được bóc, dỡ vỏ, hộp.

4. Làm việc trong Trung tâm dữ liệu

a) Quá trình vào, ra Trung tâm dữ liệu phải được ghi sổ nhật ký.

b) Dữ liệu của hệ thống camera giám sát vào, ra được lưu tối thiểu 03 tháng.

5. Phải có kế hoạch sao lưu dữ liệu hằng ngày, tự động đối với các dữ liệu quan trọng gồm: thông tin cấu hình của hệ thống mạng, máy chủ; cơ sở dữ liệu; tập tin nhật ký hoạt động (của thiết bị bảo mật, máy chủ, hệ quản trị cơ sở dữ liệu,...). Việc sao lưu phải đảm bảo khả năng phục hồi dữ liệu khi có sự cố xảy ra.

6. Hệ thống thiết bị, phần mềm an toàn, an ninh thông tin

a) Các vùng mạng, máy chủ trong Trung tâm dữ liệu phải được kiểm soát bởi tường lửa.

b) Các máy chủ phải được cài đặt phần mềm phòng chống mã độc và được quản lý thống nhất, tập trung.

c) Mọi truy cập vào ra giữa các vùng mạng, máy chủ phải có hệ thống theo dõi, giám sát và phát hiện xâm nhập.

d) Nhật ký hoạt động của thiết bị, phần mềm an toàn, an ninh thông tin phải được lưu giữ tối thiểu 03 tháng để phục vụ công tác khảo sát, phân tích hoặc điều tra khi có sự cố xảy ra.

7. Trung tâm dữ liệu phải có hệ thống điện dự phòng, hệ thống chống cháy tự động và hệ thống chống sét.

Điều 5. Quản lý kết nối

1. Kết nối mạng nội bộ

a) Đối với kết nối hữu tuyến phải đảm bảo với mỗi cổng mạng chỉ cho phép duy nhất một máy tính kết nối.

b) Tất cả máy tính đã kết nối phải được cài hệ điều hành có bản quyền hoặc hệ điều hành mã nguồn mở thuộc danh mục do Bộ Thông tin và Truyền thông ban hành đồng thời phải được đặt mật khẩu truy cập an toàn và thiết lập

chế độ tự động bảo vệ màn hình sau 5 phút không sử dụng. Mật khẩu máy tính phải được thay đổi ít nhất 3 tháng/lần.

c) Đặt tên máy theo quy ước: [Viết tắt tên Người sử dụng] + [Số phòng] + [Tên Tòa nhà]; Tên nhóm: đặt tên nhóm theo tên viết tắt của đơn vị.

d) Máy tính phải được cấu hình nhằm vô hiệu hóa tính năng tự động thực thi (autoplay) các tập tin trên các thiết bị lưu trữ di động.

e) Máy tính phải được cài đặt phần mềm phòng chống mã độc dùng chung của Bộ. Phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc khi sao chép, mở các tập tin.

2. Kết nối hệ thống thông tin nội bộ, kết nối mạng không dây

a) Mỗi cá nhân, đơn vị thuộc Bộ được cấp một tài khoản truy cập dùng cho mọi ứng dụng nội bộ của Bộ.

b) Các hệ thống thông tin cần giới hạn số lần đăng nhập sai liên tiếp vào hệ thống. Hệ thống tự động khoá tài khoản trong một khoảng thời gian nhất định trước khi tiếp tục cho đăng nhập nếu liên tục đăng nhập sai vượt quá số lần quy định.

c) Thiết bị kết nối mạng không dây phải hỗ trợ kiểu xác thực WPA2-Enterprise. Mọi đối tượng quy định tại Điều 1 khi kết nối mạng không dây phải sử dụng tài khoản truy cập được cấp. Khách đến làm việc tại Bộ chỉ được kết nối mạng không dây để truy cập internet.

Điều 6. Quản lý nâng cấp, sửa chữa, bảo trì, xử lý sự cố

1. Quá trình thực hiện nâng cấp, sửa chữa, bảo trì, xử lý sự cố phải có cán bộ giám sát trực tiếp tại nơi thực hiện. Cán bộ giám sát phải đeo thẻ làm việc.

2. Mỗi lần thực hiện nâng cấp, sửa chữa, bảo trì, xử lý sự cố phải được ghi biên bản.

3. Các ứng dụng dùng chung, hệ thống thông tin, cơ sở dữ liệu trước khi nâng cấp, sửa chữa, bảo trì, xử lý sự cố phải thực hiện sao lưu.

4. Các ứng dụng, hệ thống thông tin trực tuyến trước khi đưa vào sử dụng phải được kiểm tra bảo mật.

Điều 7. Quản lý lưu trữ, sao chép

1. Ổ cứng, thẻ nhớ, đĩa CD, DVD, băng từ,... của hệ thống lưu trữ trong Trung tâm dữ liệu, của máy tính soạn thảo, lưu trữ văn bản có tính chất mật không được thanh lý.

2. Chỉ sử dụng thiết bị lưu dữ liệu ngoài do Ban Cơ yếu Chính phủ cấp để sao chép dữ liệu thuộc danh mục bí mật Nhà nước của Bộ giữa các máy tính soạn thảo.

3. Khi kết nối thiết bị lưu dữ liệu ngoài vào máy tính, phải sử dụng phần mềm phòng chống mã độc để quét trước khi sử dụng.

Điều 8. Ứng dụng Chứng thư số

1. Cá nhân, đơn vị, tổ chức sử dụng dịch vụ chứng thực số do Tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng cung cấp.

2. Các hệ thống ứng dụng dùng chung nội bộ, hệ thống cung cấp dịch vụ công trực tuyến phải sử dụng chứng thư số để mã hóa.

3. Cá nhân, đơn vị, tổ chức sử dụng chứng thư số để ký, mã hóa văn bản.

Điều 9. Các hành vi bị nghiêm cấm

1. Tạo ra, cài đặt, phát tán phần mềm độc hại.

2. Xâm nhập, sửa đổi, xóa bỏ nội dung thông tin của đơn vị, tổ chức, cá nhân trong và ngoài Bộ.

3. Cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin.

4. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của đơn vị, tổ chức, cá nhân trong và ngoài Bộ.

5. Làm mất an toàn, bí mật thông tin của đơn vị, tổ chức, cá nhân trong và ngoài Bộ được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

6. Phát triển, cài đặt các hệ thống thử nghiệm trên hệ thống ứng dụng đang vận hành.

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

Điều 10. Trách nhiệm của các đơn vị, tổ chức thuộc Bộ

1. Thủ trưởng các đơn vị, tổ chức có trách nhiệm phổ biến, quán triệt Quy chế này đến toàn thể cán bộ, công chức, viên chức trong đơn vị, nghiêm túc tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trước Bộ trưởng trong công tác đảm bảo an toàn, an ninh thông tin tại đơn vị mình. Chủ động đăng ký, cử công chức, viên chức và người lao động trong đơn vị tham dự các lớp hướng dẫn về an toàn, an ninh thông tin do Bộ tổ chức.

2. Gửi các yêu cầu kết nối mạng nội bộ, lắp đặt mạng không dây, cấp tài khoản nội bộ tới Trung tâm Tin học.

3. Phối hợp, cung cấp thông tin và tạo điều kiện cho cán bộ kỹ thuật triển khai công tác kiểm tra khắc phục sự cố xảy ra một cách kịp thời, nhanh chóng và đạt hiệu quả.

4. Thông báo kịp thời cho Trung tâm Tin học danh sách cán bộ thuộc đơn vị mình quản lý, sử dụng khi có biến động về nhân sự để thực hiện việc chuyển quyền hoặc thu hồi các tài khoản truy cập Trung tâm Tin học đã cấp.

5. Đối với các đơn vị có sử dụng lao động hợp đồng, trong hợp đồng lao động phải có các điều khoản về trách nhiệm đảm bảo an toàn thông tin.

6. Đối với các đơn vị có hệ thống dịch vụ công phải xây dựng quy định quản lý, vận hành đảm bảo an toàn, an ninh thông tin.

7. Khi mua máy tính nếu sử dụng phần mềm hệ điều hành thương mại phải mua kèm bản quyền.

Điều 11. Trách nhiệm của cán bộ, công chức, viên chức và người lao động.

1. Thực hiện đúng các quy định tại Quy chế này.

2. Không được tự ý cài các phần mềm trên máy tính đã kết nối mạng khi chưa có sự đồng ý của người có thẩm quyền theo quy định của cơ quan. Trừ những phần mềm có tại kho lưu trữ tại địa chỉ ftp://setup.mpi.gov.vn:43122.

3. Không được gỡ bỏ phần mềm chống mã độc của Bộ ra khỏi máy tính đã kết nối mạng.

4. Không đặt chế độ tự động đăng nhập vào các hệ thống thông tin. Có trách nhiệm bảo mật tài khoản truy cập được cấp, không giao tài khoản, mật khẩu cá nhân cho người khác. Phải tắt máy tính cá nhân trước khi về.

5. Khi chia sẻ dữ liệu trực tiếp trên mạng (Network File and Folder Sharing) phải đặt mật khẩu an toàn.

6. Khi phát hiện ra bất kỳ dấu hiện nào liên quan đến việc bị nhiễm mã độc trên máy trạm (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu,...), người sử dụng phải tắt máy và báo trực tiếp cho bộ phận kỹ thuật của Trung tâm Tin học để xử lý.

7. Thực hiện sao lưu dữ liệu trên máy tính.

8. Chủ động đăng ký với lãnh đạo đơn vị về yêu cầu cấp mới tài khoản truy cập, yêu cầu được đào tạo an toàn, an ninh thông tin.

9. Chủ động cập nhật các chính sách, thủ tục mới quy định về an toàn, an ninh thông tin.

10. Không dùng các biện pháp kỹ thuật để truy cập vào các địa chỉ trên mạng đã bị ngăn chặn.

Điều 12. Trách nhiệm của Trung tâm Tin học

1. Thực hiện đúng các quy định liên quan tại Quy chế này.

2. Tham mưu cho Bộ trưởng về công tác đảm bảo an toàn, an ninh thông tin; Thành lập bộ phận phụ trách công tác an toàn, an ninh thông tin.

3. Cấp, hủy tài khoản, quyền truy cập các hệ thống thông tin đối với các cá nhân, đơn vị; cấp, tổ chức cấp, hủy chứng thư số, thẻ nhớ an toàn của Ban cơ yếu Chính phủ.

4. Thực hiện kết nối máy tính vào mạng nội bộ Bộ Kế hoạch và Đầu tư.

5. Thiết kế, lựa chọn giải pháp công nghệ, triển khai xây dựng và cấu hình hệ thống an toàn, an ninh mạng của Bộ: tường lửa, hệ thống phát hiện xâm nhập, hệ thống chống xâm nhập, hệ thống quản lý nhật ký tập trung, hệ thống phòng chống mã độc tập trung,...

6. Lập Kế hoạch kiểm tra, rà soát, đánh giá tình trạng an toàn, an ninh thông tin. Chủ trì việc kiểm tra bảo mật các ứng dụng, hệ thống thông tin trực tuyến trước khi đưa vào sử dụng.

7. Chủ trì phối hợp với các cơ quan quản lý nhà nước trong việc xử lý, ứng cứu sự cố an toàn, an ninh thông tin. Thực hiện nghĩa vụ thành viên của mạng lưới ứng cứu sự cố mạng Internet Việt Nam.

8. Thực hiện việc ghi nhật ký các thiết bị mạng; máy chủ; cơ sở dữ liệu; thiết bị, phần mềm bảo mật và lưu trữ theo nguyên tắc sau:

a) Các nhật ký này phải được bảo vệ an toàn nhằm phục vụ công tác kiểm tra, phân tích khi cần thiết.

b) Các sự kiện tối thiểu cần phải được ghi nhật ký gồm: quá trình đăng nhập hệ thống; tạo, cập nhật hoặc xóa dữ liệu; các hành vi xem, thiết lập cấu hình hệ thống; việc thiết lập các kết nối bất thường vào và ra hệ thống; thay đổi quyền truy cập hệ thống...

9. Thực hiện việc theo dõi nhật ký của hệ thống và các sự kiện khác có liên quan để đánh giá, cảnh báo, báo cáo các rủi ro và mức độ nghiêm trọng các rủi ro. Hỗ trợ kỹ thuật cho các đơn vị, tổ chức, cá nhân về an toàn, an ninh mạng, máy tính.

10. Tổ chức thực hiện việc trực quản lý vận hành, an toàn, an ninh mạng.

11. Xây dựng các tài liệu hướng dẫn sử dụng mạng, máy tính, các hệ thống ứng dụng dùng chung an toàn, bảo mật. Lập kế hoạch và tổ chức phổ biến tuyên truyền, đào tạo.

12. Xây dựng các quy trình :

a) Quản lý vận hành các hệ thống bảo mật, mạng, Trung tâm dữ liệu, các hệ thống thông tin dùng chung đảm bảo an toàn, an ninh thông tin.

b) Các kịch bản chống, phản ứng, khắc phục sự cố các dạng tấn công qua mạng.

c) Thu thập, biên tập, cập nhật, kiểm duyệt, xuất bản thông tin an toàn đối với Cổng thông tin điện tử của Bộ, các hệ thống thông tin dùng chung của Bộ, các trang thông tin được Bộ giao quản trị nội dung.

13. Thực hiện chế độ báo cáo, bao gồm:

a) Báo cáo vào tháng 12 hằng năm về tình trạng an toàn an ninh thông tin.

b) Báo cáo khi có sự cố an toàn an ninh thông tin và không thể tự khắc phục (quá tải, mất kiểm soát, mất thiết bị,...) hoặc khi có yêu cầu của cơ quan quản lý nhà nước.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 13. Khen thưởng và xử lý vi phạm

1. Hằng năm, Trung tâm Tin học dựa trên các điều tra, giám sát để xác lập bảng xếp hạng an toàn, an ninh thông tin của các đơn vị thuộc Bộ, báo cáo Lãnh

đạo Bộ, đồng thời gửi Vụ Thi đua khen thưởng làm cơ sở đề xuất Bộ trưởng khen thưởng theo quy định hiện hành.

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

Điều 14. Điều khoản thi hành

1. Trung tâm Tin học chủ trì, phối hợp với các cơ quan, tổ chức, đơn vị có liên quan tổ chức hướng dẫn, theo dõi và kiểm tra việc thực hiện các quy định của Quy chế này.

2. Trong quá trình thực hiện Quy chế này, nếu có vướng mắc, phát sinh cần sửa đổi, bổ sung đề nghị thông báo Trung tâm Tin học biết để tổng hợp, trình Bộ trưởng xem xét, quyết định cho phù hợp với điều kiện thực tế và quy định của pháp luật hiện hành./.

BỘ TRƯỞNG

Bùi Quang Vinh