BỘ VĂN HÓA, THỂ THAO VÀ DU LỊCH	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Số: 3655 /BVHTTDL-KHCNMT V/v Hướng dẫn đảm bảo an toàn thông tin trong cơ quan, đơn vị trực thuộc Bộ.	**Độc lập - Tự do - Hạnh phúc** *Hà Nội, ngày 01 tháng 9 năm 2015*

Kính gửi: Cơ quan, đơn vị trực thuộc Bộ Văn hóa, Thể thao và Du lịch.

Nhằm đảm bảo an toàn thông tin trong hoạt động, ứng dụng và phát triển công nghệ thông tin của Bộ Văn hóa, Thể thao và Du lịch, Bộ đã gửi các cơ quan, đơn vị trực thuộc Bộ *(gọi tắt là đơn vị)* Công văn số 1198 /BVHTTDL-KHCNMT ngày 31 tháng 3 năm 2015 về việc đôn đốc tăng cường đảm bảo an toàn thông tin trong các cơ quan, đơn vị thuộc Bộ. Trong khi chờ ban hành Quy chế Bảo đảm an toàn thông tin của Bộ, đề nghị các đơn vị tiếp tục thực hiện các nội dung của Công văn số 1198/BVHTTDL-KHCNMT và áp dụng thêm Hướng dẫn này về công tác bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin tại đơn vị với các nội dung sau:

1. Phạm vi, chủ thể an toàn thông tin:

1.1. Máy tính: là máy tính cá nhân phục vụ công việc, được đơn vị trang bị để thực hiện nhiệm vụ, công việc của đơn vị.

1.2. Thiết bị, hạ tầng công nghệ thông tin: là hệ thống thiết bị, máy móc công nghệ thông tin *của phòng máy chủ* như thiết bị chống sét, phòng cháy, chữa cháy, các thiết bị chuyển mạch, định tuyến, tường lửa...; *của mạng nội bộ* (LAN) có dây và không dây.

1.3. Cổng thông tin điện tử/trang thông tin điện tử của đơn vị: là Cổng (hoặc trang) thông tin điện tử của Bộ (hoặc của đơn vị) có thông tin đáp ứng Nghị định số 43/2011/NĐ-CP ngày 13 tháng 6 năm 2011 của Chính phủ quy định về việc cung cấp thông tin và dịch vụ công trực tuyến trên trang thông tin điện tử hoặc Cổng thông tin điện tử của cơ quan nhà nước.

1.4. Tệp (file) dữ liệu: là nội dung số dạng file được đơn vị tạo lập trong quá trình thực hiện công việc theo chức năng, nhiệm vụ, quyền hạn được cấp có thẩm quyền quy định.

1.5. Dữ liệu của hệ thống thông tin: là dữ liệu được tạo lập trong quá trình sử dụng phần mềm của đơn vị; dữ liệu của hệ thống thông tin được sử dụng và lưu trữ trên hệ thông tin cơ sở dữ liệu (data base) theo các mô hình khác nhau (trên local, client-server, cloud...). Đơn vị chủ động xác định dữ liệu của hệ thống thông tin cần đảm bảo an toàn.

1.6. Tài khoản người dùng: là *tài khoản thư điện tử công vụ* của cá nhân, đơn vị và các *tài khoản khác xác thực người dùng* của đơn vị (như chứng thư số, chữ ký số, tài khoản web server, mail server, tài khoản ACP hosting, CMS...), thường bao gồm: tên người dùng (user) và mật khẩu (password).

2. Yêu cầu về an toàn

Tùy thuộc hiện trạng các chủ thể và mô hình quản lý (là thuê dịch vụ công nghệ thông tin hoặc đơn vị chủ động hoàn toàn/một phần) để thủ trưởng đơn vị lựa chọn giải pháp phù hợp, ngoài một số yêu cầu bắt buộc, đơn vị đảm bảo hiệu quả tối đa các yêu cầu sau:

2.1. Máy tính phải được cài đặt ít nhất 01 phần mềm diệt virus (thường xuyên cập nhật phiên bản mới) có khả năng phòng ngừa, an toàn trước virus máy tính lây nhiễm qua mạng máy tính, mạng internet, thiết bị kết nối ngoại vi qua các cổng thông dụng như USB, cổng mạng...

2.2. Thiết bị, hạ tầng công nghệ thông tin: Đảm bảo an toàn về mặt vật lý, chống cháy, nổ, chập điện, chống sét...

2.3. Cổng thông tin điện tử/trang thông tin điện tử phải hoạt động bình thường, liên tục, không bị gián đoạn bởi các cuộc tấn công có chủ đích với ý đồ xấu. Trường hợp đơn vị thuê dịch vụ công nghệ thông tin phải thể hiện điều khoản này ở hợp đồng cung cấp dịch vụ.

2.4. File dữ liệu: phải được đảm bảo *tính an toàn* (không bị mất), *toàn vẹn* (không bị thay đổi nội dung khi lưu trữ), *tính xác thực* (đúng với nguồn gốc người tạo lập/lưu trữ/gửi), *tính sẵn sàng* (có thể sử dụng được bất kỳ lúc nào).

2.5. Dữ liệu của hệ thống thông tin: tùy thuộc mô hình ứng dụng của hệ thống thông tin (trên local, client-server, cloud ...) để chọn giải pháp lưu trữ, dự phòng đảm bảo an toàn các *file dữ liệu* của hệ thống thông tin.

2.6. Tài khoản người dùng bao gồm user và password phải được bảo quản cẩn thận. Mật khẩu (password) phải được đặt với độ khó/độ mạnh cao; mật khẩu nên đồng thời chứa chữ cái, chữ số và ký tự đặc biệt như @, #, $, %, &, *, +... ; khuyến khích thay đổi mật khẩu định kỳ theo (1, 3, 6...) tháng.

Đối với cán bộ, công chức, viên chức và người lao động chuyển công tác hoặc chấm dứt hợp đồng lao động, đơn vị phải hủy tài khoản người dùng, quyền truy cập các hệ thống thông tin và các tài sản liên quan đến quản lý, truy cập hệ thống thông tin như khóa, thẻ nhận dạng, thư mục lưu trữ dữ liệu...

3. Mức độ, phạm vi và phương án xử lý sự cố

3.1. Phân loại mức độ sự cố an toàn, an ninh thông tin

Căn cứ vào yêu cầu an toàn ở *Mục 2* và ảnh hưởng của sự cố đến hoạt động của đơn vị, có thể phân loại mức độ sự cố an toàn, an ninh thông tin như sau:

a) Mức thấp: Ảnh hưởng đến công việc của cá nhân, không gây gián đoạn hay đình trệ công việc của đơn vị.

b) Mức trung bình: Ảnh hưởng đến một nhóm người (phòng, ban...) không gây gián đoạn hay đình trệ công việc của đơn vị.

c) Mức cao: Ảnh hưởng đến một trong các hoạt động chính của cơ quan, có thể gây đình trệ một phần công việc của đơn vị.

d) Mức khẩn cấp: Ảnh hưởng nghiêm trọng, gây tê liệt đến hoạt động ứng dụng công nghệ thông tin của đơn vị.

3.2. Phạm vi sự cố thuộc trách nhiệm của các đơn vị

- Các đơn vị chủ động đảm bảo an toàn và xử lý các mức độ sự cố *(tại mục 3.1)* thuộc chủ thể an toàn thông tin quy định tại *Mục 1*.

- Với các chủ thể an toàn thông tin thuộc quyền quản lý của đơn vị nhưng được cung cấp dưới dạng dịch vụ công nghệ thông tin, đơn vị chủ động rà soát và có giải pháp thích hợp.

3.3. Phạm vi sự cố thuộc trách nhiệm của đơn vị đầu mối

Trong trường hợp, sự cố (ở *Mức cao* trở lên) gây mất an toàn thông tin của đơn vị, vượt khả năng xử lý và tầm kiểm soát, đơn vị phải kịp thời cấp báo sớm nhất có thể (bằng điện thoại và văn bản) đến đơn vị đầu mối để phối hợp xử lý.

3.4. Sự cố phải phối hợp với cơ quan đặc biệt về an toàn thông tin

Nếu các sự cố gây mất an toàn thông tin vượt khả năng xử lý và tầm kiểm soát của đơn vị đầu mối, các đơn vị đầu mối phối hợp với đơn vị xảy ra sự cố kịp thời cấp báo với Bộ Văn hóa, Thể thao và Du lịch (qua Vụ Khoa học, Công nghệ và Môi trường) để có phương án hỗ trợ đơn vị đầu mối tổ chức xử lý kịp thời.

4. Đơn vị đầu mối trong xử lý sự cố gây mất an toàn thông tin

Khi có phát hiện được nguy cơ có thể gây mất an toàn, an ninh thông tin, bộ phận được giao quản lý công nghệ thông tin, an toàn thông tin của đơn vị phải chủ động báo cáo Lãnh đạo cơ quan nhằm kịp thời kiểm soát, hạn chế thiệt hại.

Các đơn vị chủ động phát hiện, xử lý sự cố trong phạm vi và trách nhiệm tại *Mục 3.2*. Trong trường hợp cần thiết và có yêu cầu hỗ trợ của đơn vị, các đầu mối chịu trách nhiệm hỗ trợ, phối hợp với đơn vị có xảy ra sự cố để đánh giá mức độ mất an toàn, kịp thời lựa chọn phương án khắc phục.

Các đầu mối tiếp nhận xử lý sự cố, tổng hợp tình hình an toàn, an ninh thông tin trong phạm vi phối hợp, hỗ trợ đơn vị như sau:

4.1. Văn phòng Bộ: Các đơn vị trong khối trụ sở 51 Ngô Quyền.

4.1. Trung tâm Thông tin thể thao (Tổng cục Thể dục thể thao): Khối cơ quan Tổng cục Thể dục thể thao, các đơn vị sự nghiệp trực thuộc.

4.3. Trung tâm Thông tin Du lịch (Tổng cục Du lịch): Khối cơ quan Tổng cục Du lịch, các đơn vị sự nghiệp trực thuộc.

4.4. Trung tâm Công nghệ thông tin: Các đơn vị trực thuộc Bộ, không bao gồm: Tổng cục Thể dục thể thao, Tổng cục Du lịch, các đơn vị trong khối trụ sở 51 Ngô Quyền.

5. Các văn bản liên quan có thể tham khảo

- Thông tư số 22/2013/TT-BTTTT ngày 23 tháng 12 năm 2013 của Bộ Thông tin và Truyền thông ban hành Danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước;

- Công văn số 430/BTTTT-CATTT ngày 09 tháng 02 năm 2015 của Bộ Thông tin và Truyền thông hướng dẫn bảo đảm an toàn thông tin cho hệ thống thư điện tử của cơ quan, tổ chức nhà nước;

- Nghị định số 43/2011/NĐ-CP ngày 13 tháng 6 năm 2011 của Chính phủ quy định về việc cung cấp thông tin và dịch vụ công trực tuyến trên trang thông tin điện tử hoặc Cổng thông tin điện tử của cơ quan nhà nước;

- Công văn số 1198 /BVHTTDL-KHCNMT ngày 31 tháng 3 năm 2015 của Bộ Văn hóa, Thể thao và Du lịch về việc đôn đốc tăng cường đảm bảo an toàn thông tin trong các cơ quan, đơn vị thuộc Bộ.

Bản mềm Công văn này và các văn bản liên quan được đăng tải trên trang thông tin điện tử của Vụ Khoa học, Công nghệ và Môi trường (mục ***"Công văn, Thông báo"*** địa chỉ http://khcnmt-bvhttdl.vn).

6. Tổ chức thực hiện và chế độ báo cáo

6.1. Thủ trưởng đơn vị chịu trách nhiệm về an toàn thông tin của đơn vị; khuyến cáo người sử dụng, phân công cán bộ quản lý về an toàn thông tin (ưu tiên cán bộ có bằng cấp/chuyên môn về Công nghệ thông tin) và bố trí đủ nguồn lực có chất lượng phù hợp quy mô nhằm bảo đảm an ninh, an toàn thông tin; định kỳ hoặc đột xuất kiểm tra việc thực hiện an toàn thông tin tại đơn vị.

Các đơn vị đăng ký danh sách đầu mối quản lý, chuyên trách/phụ trách về công nghệ thông tin *(cập nhật lại,thời điểm tháng 8 năm 2015)*, an toàn thông tin của đơn vị ở *Phụ lục (kèm theo)*, gửi về Bộ Văn hóa, Thể thao và Du lịch (qua Vụ Khoa học, Công nghệ và Môi trường) **trước ngày 10 tháng 9 năm 2015.**

6.2. Chế độ báo cáo

Định kỳ hoặc đột xuất, đơn vị chủ động báo cáo tình hình an toàn thông tin và xử lý sự cố (nếu có) tại đơn vị, gửi đầu mối để tổng hợp.

Vụ Khoa học, Công nghệ và Môi trường căn cứ tổng hợp của các đầu mối để xây dựng báo cáo định kỳ hoặc đột xuất theo yêu cầu, trình Lãnh đạo Bộ.

Trong quá trình thực hiện Công văn này, nếu gặp vướng mắc cần hỗ trợ đề nghị đơn vị liên hệ Bộ Văn hóa, Thể thao và Du lịch (qua Vụ Khoa học, Công nghệ và Môi trường - Chuyên viên Dương Viết Huy, *điện thoại: 0914.696.456; email: duongviethuy-vhttdl@chinhphu.vn)./.*

Nơi nhận:
- Như trên;
- Bộ trưởng *(để báo cáo);*
- Thứ trưởng Đặng Thị Bích Liên *(để báo cáo);*
- Lưu: VT, KHCNMT, VH.90.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

(đã ký)

Đặng Thị Bích Liên

BỘ VĂN HÓA, THỂ THAO VÀ DU LỊCH

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

Phụ lục
DANH SÁCH ĐẦU MỐI QUẢN LÝ CÔNG NGHỆ THÔNG TIN, AN TOÀN THÔNG TIN CỦA ĐƠN VỊ
(Ban hành kèm theo Công văn số 3655/BVHTTDL-KHCNMT ngày 01 tháng 9 năm 2015 của Bộ Văn hóa, Thể thao và Du lịch)

STT	***Họ và tên***	***Chức vụ/Vai trò***	***Số điện thoại***	***Email công vụ*** (*)	***Ghi chú*** (**)
1		Thủ trưởng			**Bắt buộc** phải đăng ký
2		Lãnh đạo phụ trách CNTT			Nếu có (ngoài thủ trưởng)
3		CV phụ trách/chuyên trách CNTT			**Bắt buộc** phải đăng ký
4		CV phụ trách/chuyên trách CNTT			Nếu có thêm
5		.....			Nếu có thêm
6		CV chuyên trách về an toàn thông tin			**Bắt buộc** phải đăng ký
7		.....			Nếu có thêm
8		.....			Nếu có thêm

(*): Email công vụ sẽ được sử dụng để xác thực (bên gửi, bên nhận) trong quá trình trao đổi văn bản điện tử qua email.

(**): Một cán bộ/chuyên viên có thể phụ trách/chuyên trách đồng thời công nghệ thông tin và an toàn thông tin.