CỤC HÀNG KHÔNG VIỆT NAM
CẢNG VỤ HK MIỀN TRUNG

Số: 230 /QĐ-CVMT

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

Đà Nẵng, ngày 09 tháng 9 năm 2024

QUYẾT ĐỊNH
Ban hành Quy định bảo đảm an toàn thông tin, an ninh mạng tại Cảng vụ Hàng không miền Trung

GIÁM ĐỐC CẢNG VỤ HÀNG KHÔNG MIỀN TRUNG

Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19/11/2015;

Căn cứ Luật An ninh mạng số 24/2018/QH14 ngày 12/6/2018;

Căn cứ Nghị định số 53/2022/NĐ-CP ngày 15/08/2022 của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng

Căn cứ Quyết định số 724/QĐ-BGTVT ngày 13/06/2024 của Bộ Giao thông vận tải về việc ban hành Quy chế bảo đảm an toàn thông tin, an ninh mạng Bộ GTVT;

Căn cứ Quyết định số 2075/QĐ-BGTVT ngày 09/07/2007 của Bộ Giao không vận tải về việc thành lập Cảng vụ Hàng không miền Trung;

Căn cứ Quyết định số 3424/QĐ-BGTVT ngày 12/12/2017 của Bộ Giao thông vận tải quy định chức năng nhiệm vụ, quyền hạn và cơ cấu tổ chức của Cảng vụ Hàng không miền Trung;

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

QUYẾT ĐỊNH

Điều 1. Ban hành kèm theo quyết định này Quy định **" Đảm bảo an toàn thông tin, an ninh mạng tại Cảng vụ Hàng không miền Trung"**

Điều 2: Quyết định này có hiệu lực kể từ ngày ký. Trưởng phòng Tổ chức – Hành chính, thủ trưởng các phòng, các đại diện CVHK trực thuộc Cảng vụ Hàng không miền Trung và các cá nhân liên quan chịu trách nhiệm thi hành quyết định này./.

Nơi nhận:
- Ban Giám đốc;
- Như điều 2;
- Lưu VT, TCHC (Dg.[16b])

GIÁM ĐỐC

BỘ GIAO THÔNG VẬN TẢI
CẢNG VỤ HÀNG KHÔNG MIỀN TRUNG
CỤC HÀNG KHÔNG VIỆT NAM

Bùi Văn Thành

CỤC HÀNG KHÔNG VIỆT NAM
CẢNG VỤ HK MIỀN TRUNG

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

Đà Nẵng, ngày 09 tháng 09 năm 2024

QUY ĐỊNH
Đảm bảo an toàn thông tin, an ninh mạng tại Cảng vụ Hàng không miền Trung

(Ban hành kèm theo Quyết định số 230/QĐ-CVMT ngày 09/ 09 /2024 của Giám đốc Cảng vụ HK miền Trung)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy định này quy định việc đảm bảo an toàn thông tin, an ninh mạng trong hoạt động ứng dụng công nghệ thông tin và Chuyển đổi số của Cảng vụ Hàng không miền Trung (gọi là Cảng vụ HKMT).

Điều 2. Đối tượng áp dụng

Quy định này được áp dụng đối với các phòng, các đại diện Cảng vụ HKMT; các cán bộ, viên chức và người lao động trực thuộc Cảng vụ HKMT trong việc quản lý, vận hành, khai thác, sử dụng và đảm bảo an toàn thông tin, an ninh mạng đối với hệ thống thông tin, hệ thống mạng, hệ thống máy tính của Cảng vụ HKMT.

Điều 3. Giải thích từ ngữ

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

1. Hệ thống thông tin (HTTT) là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên mạng của một cơ quan, tổ chức.

2. Chủ quản hệ thống thông tin là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin.

3. Đơn vị vận hành hệ thống thông tin là đơn vị được chủ quản hệ thống thông tin giao nhiệm vụ vận hành hệ thống thông tin. Trong trường hợp chủ quản hệ thống thông tin thuê ngoài dịch vụ công nghệ thông tin, đơn vị vận hành hệ thống thông tin là bên cung cấp dịch vụ.

4. An toàn thông tin mạng là sự bảo vệ thông tin số và các hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

5. An ninh mạng là việc bảo đảm thông tin trên mạng không gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước, quyền và lợi ích

hợp pháp của tổ chức, cá nhân.

6. Phần mềm độc hại là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

7. Mạng nội bộ (LAN - Local Area Network): là một hệ thống mạng bao gồm các máy tính và các thiết bị ngoại vi được liên kết với nhau. Người sử dụng mạng nội bộ có thể chia sẻ tài nguyên như thông tin, dữ liệu, các phần mềm dùng chung, các ứng dụng chuyên ngành, các công cụ tiện ích và các thiết bị ngoại vi như máy in...

8. Cán bộ chuyên trách, kiêm nhiệm là viên chức, người lao động được tuyển dụng phụ trách công nghệ thông tin tại cơ quan, đơn vị.

Điều 4. Nguyên tắc bảo đảm an toàn thông tin, an ninh mạng

1. Bảo đảm an toàn thông tin, an ninh mạng là yêu cầu bắt buộc, tuân thủ các nguyên tắc chung quy định tại Điều 4 Luật An toàn thông tin mạng, Điều 4 Luật An ninh mạng và các quy định pháp luật khác có liên quan.

2. Giám đốc Cảng vụ HKMT chịu trách nhiệm chỉ đạo thực hiện các nhiệm vụ bảo đảm an toàn thông tin, an ninh mạng tại đơn vị; Phối hợp; giúp đỡ, tạo điều kiện cho cơ quan, tổ chức và người có trách nhiệm tiến hành các biện pháp bảo vệ an ninh mạng.

3. Các phòng chuyên môn, các đại diện, cán bộ, viên chức và người lao động có trách nhiệm bảo đảm an toàn thông tin, an ninh mạng. Hoạt động an toàn thông tin mạng của các phòng chuyên môn, các tổ chức đoàn thể, các cá nhân phải đúng quy định của pháp luật, bảo đảm quốc phòng, an ninh quốc gia, bí mật nhà nước, giữ vững ổn định chính trị, trật tự, an toàn xã hội và thúc đẩy phát triển kinh tế - xã hội.

4. Các phòng chuyên môn, các tổ chức đoàn thể, các cá nhân không được xâm phạm an toàn thông tin, an ninh mạng của tổ chức, cá nhân khác.

5. Việc xử lý sự cố an toàn thông tin, an ninh mạng phải bảo đảm quyền và lợi ích hợp pháp của tổ chức, cá nhân, không xâm phạm đến đời sống riêng tư, bí mật cá nhân, bí mật gia đình của cá nhân, thông tin riêng của tổ chức.

6. Hoạt động an toàn thông tin, an ninh mạng phải được thực hiện thường xuyên, liên tục, kịp thời và hiệu quả.

7. Thông tin mật, thông tin thuộc Danh mục bí mật nhà nước phải được bảo vệ theo quy định của Nhà nước, quy định của đơn vị về công tác bảo vệ bí mật Nhà nước và các nội dung tương ứng trong Quy định này.

Chương II
QUY ĐỊNH ĐẢM BẢO AN TOÀN THÔNG TIN, AN NINH MẠNG

Điều 5. Bảo vệ bí mật nhà nước trong hoạt động ứng dụng công nghệ thông tin

1. Quy định về soạn thảo, in ấn, phát hành và sao chụp tài liệu mật

a. Không được sử dụng máy tính nối mạng Internet để soạn thảo văn bản; chuyển giao, lưu trữ thông tin có nội dung thuộc bí mật nhà nước (gọi là BMNN). Không cung cấp hoặc gửi tin, tài liệu thông tin bí mật nhà nước trên Cổng/Trang thông tin điện tử; trên hệ thống quản lý văn bản của Cảng vụ HKMT, trên hệ thống Mail online của Cảng vụ HKMT.

b. Không được in, sao chụp tài liệu bí mật nhà nước trên các thiết bị kết nối mạng internet;

c. Phải bố trí 01 máy vi tính riêng, không kết nối mạng nội bộ và mạng Internet dùng để quản lý, soạn thảo các tài liệu mật của nhà nước theo quy định.

d. Khi sửa chữa, khắc phục các sự cố của máy tính dùng soạn thảo văn bản mật, bộ phận được giao nhiệm vụ quản lý máy tính mật phải báo cáo cho người có thẩm quyền. Không được cho phép các tổ chức, cá nhân không có trách nhiệm trực tiếp sửa chữa, xử lý, khắc phục sự cố đối với máy tính này.

2. Trước khi thanh lý các máy tính phục vụ công tác BMNN, đơn vị vận hành chuyên trách công nghệ thông tin phải dùng các biện pháp kỹ thuật xoá bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính. Báo cáo lãnh đạo thực hiện thanh lý theo quy định.

Điều 6. Quy định về quản lý các tài khoản truy cập vào hệ thống thông tin (HTTT) và mạng nội bộ

1. Trách nhiệm, quyền hạn người dùng khi truy cập, đăng nhập các HTTT, đảm bảo mỗi người dùng khi sử dụng hệ thống thông tin phải sử dụng tài khoản truy cập với định danh duy nhất gắn với người dùng đó. Trường hợp sử dụng tài khoản dùng chung của đơn vị như mail, phải xác định các cá nhân có trách nhiệm quản lý tài khoản. Người dùng chỉ được truy cập các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình và có trách nhiệm bảo mật tài khoản truy cập được cấp.

2. Cán bộ chuyên trách, người sử dụng thực hiện quản lý tài khoản cá nhân được cấp. Người sử dụng thay đổi mật khẩu ngay sau khi đăng nhập lần đầu tiên và bảo vệ thông tin của tài khoản theo quy định.

3. Mật mã đăng nhập, truy cập hệ thống thông tin phải có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số hoặc ký tự đặc biệt như !, @, #, $, %,...). Thay đổi mật khẩu định kỳ 3 tháng 1 lần

4. Các tài khoản sử dụng các hệ thống thông tin của Cảng vụ HKMT phải tuân thủ các quy chế về quản lý sử dụng các hệ thống nêu trên.

Điều 7. Bảo đảm an toàn hạ tầng mạng

1. Quản lý hạ tầng mạng nội bộ

a. Thiết bị CNTT được trang bị tại các phòng chuyên môn, các đại diện là tài sản của Nhà nước, được quản lý, sử dụng theo quy định của Nhà nước. Các phòng chuyên môn, cán bộ, viên chức và người lao động có trách nhiệm quản lý trang thiết bị được giao sử dụng.

b. Phòng Tổ chức - Hành chính là đơn vị chủ trì làm công tác quản trị mạng nội bộ, mạng máy tính, hỗ trợ kỹ thuật và duy trì hoạt động của hệ thống thông tin của Cảng vụ HKMT; kiểm tra hiện trạng, đề xuất sửa chữa hoặc mua mới các chủng loại thiết bị CNTT phù hợp, an toàn, bảo mật theo quy định về quản lý, sử dụng tài sản cơ quan nhà nước.

c. Các phòng, các đại diện và cá nhân tham gia vào hệ thống mạng nội bộ tại đơn vị không được tự ý thay đổi những thông số mạng hay tự ý đưa các thiết bị mạng khác tham gia vào hệ thống mạng nội bộ. Không được tự ý cài đặt các phần mềm, ứng dụng không phục vụ công việc vào hệ thống mạng này.

Điều 8. Bảo đảm an toàn dữ liệu trong hệ thống mạng

1. Quản lý tài khoản và chữ ký số

a. Chủ tài khoản, chữ ký số không chia sẻ, giao quyền tài khoản, chữ ký số và mật khẩu truy nhập cho người khác. Không sử dụng tài khoản của người khác (ví dụ tài khoản thư điện tử, chữ ký số, chứng thư số) để đăng nhập vào hệ thống thông tin, cơ sở dữ liệu;

b. Tài khoản thư điện tử, chữ ký số chuyên dùng (xxx@maa.gov.vn và chữ ký số do Ban Cơ yếu Chính phủ cấp) để phục vụ cho các hoạt động mang tính công vụ, không sử dụng để giao dịch, đăng ký trên mạng xã hội, các trang thông tin điện tử công cộng khác;

c. Tài khoản quản trị hệ thống thông tin (HTTT) được giao cho cán bộ, viên chức chuyên trách mảng công nghệ thông tin phục vụ cho công tác quản trị, phân quyền, cấu hình hệ thống đó. Người quản trị hệ thống không sử dụng cùng một mật khẩu cho nhiều tài khoản khác nhau;

d. Khi cá nhân thay đổi vị trí công tác, chuyển công tác, thôi việc, nghỉ hưu, ngay từ thời điểm Quyết định có hiệu lực, phòng Tổ chức - Hành chính thông báo cho bộ phận, viên chức vận hành hệ thống để điều chỉnh, thu hồi, hủy bỏ tài khoản, chữ ký số, chứng thư số.

e. Các cá nhân sử dụng các thiết bị lưu trữ dữ liệu di động (máy tính xách tay, thiết bị số cầm tay, thẻ nhớ USB, ổ cứng ngoài, đĩa...) để lưu thông tin dữ liệu công vụ có trách nhiệm bảo vệ các thiết bị này và thông tin lưu trên thiết bị, tránh làm mất, lộ thông tin; không mang ra nước ngoài thông tin của cơ quan, Nhà nước không liên quan tới nội dung công việc thực hiện ở nước ngoài. Nghiêm cấm sử dụng thiết bị do cá nhân tự trang bị để lưu giữ thông tin bí mật Nhà nước.

2. Hạn chế chia sẻ dữ liệu trên máy tính trong hệ thống mạng nội bộ. Các phòng chuyên môn, viên chức và người lao động phải sử dụng mật khẩu để bảo vệ thông tin, dữ liệu trên máy tính; không thực hiện chia sẻ toàn bộ ổ cứng; theo dõi, giám sát để kết thúc chia sẻ tài nguyên ngay khi hoàn thành.

3. Phòng Tổ chức - Hành chính quản lý việc sửa chữa hệ thống mạng nội bộ tại đơn vị. Đảm bảo thiết bị lưu trữ khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài cơ quan phải tháo rời bộ phận lưu trữ khỏi thiết bị và để lại cơ quan hoặc xóa dữ liệu lưu trữ trên thiết bị. Khi thanh lý thiết bị phải xóa dữ liệu lưu trữ vĩnh viễn bằng phần mềm hoặc thiết bị hủy dữ liệu chuyên dụng.

4. Thông tin, dữ liệu thuộc phạm vi BMNN, phải được quản lý theo quy định hiện hành về bảo vệ BMNN (theo điều 5 của quy chế này)

Chương III
QUẢN LÝ VÀ SỬ DỤNG HTTT VÀ MẠNG NỘI BỘ

Điều 9. Thông tin, dịch vụ và trao đổi thông tin trên HTTT và mạng nội bộ

1. Các loại thông tin trên HTTT và mạng nội bộ của Cảng vụ HKMT:

- Thông tin được cung cấp từ Internet.
- Thông tin từ Website Cảng vụ HKMT.
- Thông tin từ hệ thống quản lý văn bản PO.
- Thông tin từ hệ thống Mail Online.
- Thông tin từ hệ thống Truyền hình trực tuyến

2. Trao đổi thông tin trên HTTT và mạng nội bộ :

Việc trao đổi thông tin trên HTTT và mạng nội bộ phải tuân thủ các quy định hiện hành của nhà nước và các quy chế quản lý hoạt động của các HTTT do Cảng vụ HKMT ban hành

Các thông tin và dịch vụ bị cấm đưa lên HTTT và mạng nội bộ:

- Thông tin của các tổ chức chính quyền, đoàn thể, các cơ quan chức năng được yêu cầu giữ bí mật;

- Thông tin cá nhân như: tài sản cá nhân, đời tư; thông tin vi phạm quyền sở hữu trí tuệ;

- Thông tin làm ảnh hưởng đến an ninh quốc gia;

- Thông tin xuyên tạc, tuyên truyền chống đối các chủ trương chính sách của Đảng và Nhà nước, phá hoại khối đại đoàn kết dân tộc;

- Những thông tin có nội dung kích động bạo lực, truyền bá tư tưởng phản động;

- Thông tin trái với thuần phong mỹ tục như, thông tin có nội dung không lành mạnh;

- Thông tin quấy rối cá nhân, xúc phạm danh dự, vu khống, xúc phạm đến nhân phẩm công dân;

- Những thông tin và các ứng dụng có tính chất phá hoại như phát tán virus máy tính, lấy cắp thông tin, phá hoại cơ sở dữ liệu, làm tê liệt mạng máy tính.

- Thông tin có ảnh hưởng xấu đến văn hoá 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 nhảm ảnh hưởng đến uy tín của Quốc gia;

- Thông tin và các dịch vụ không được phép sử dụng theo quy định hiện hành của pháp luật.

Điều 10. Bảo đảm an toàn, an ninh thông tin các HTTT, mạng nội bộ.

1. Đối với HTTT được thuê dịch vụ vận hành quản trị hệ thống

- Xác định rõ trách nhiệm, quyền hạn và nghĩa vụ của các bên về an toàn thông tin, an ninh mạng khi ký hợp đồng. Hợp đồng với bên dịch vụ phải bao gồm các điều khoản về việc xử lý vi phạm và trách nhiệm bồi thường thiệt hại của bên dịch vụ gây ra. Yêu cầu bên dịch vụ ký và thực hiện cam kết bảo mật thông tin cả trong quá trình triển khai và sau khi hoàn tất hợp đồng.

- Đơn vị không được thuê bên dịch vụ thực hiện toàn bộ công việc quản trị (chỉnh sửa cấu hình, dữ liệu….) đối với các hệ thống thông tin quan trọng. Cung cấp, thông báo, phối hợp và yêu cầu bên dịch vụ thực hiện các quy định của đơn vị về an toàn bảo mật hệ thống thông tin (theo nghị định 85/2016/NĐ-CP ngày 01/7/2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ).

- Đảm bảo triển khai, duy trì các biện pháp an toàn thông tin, an ninh mạng do bên dịch vụ cung cấp theo đúng thỏa thuận.

2. Trách nhiệm của đơn vị cung cấp dịch vụ vận hành HTTT, cho Cảng vụ Hàng không miền Trung thuê hệ thống

- Ký và thực hiện cam kết bảo mật thông tin cả trong quá trình triển khai và sau khi hoàn tất hợp đồng. Bàn giao tài sản, quyền truy cập hệ thống thông tin do bên ký kết hợp đồng cung cấp khi hoàn thành công việc hoặc kết thúc hợp đồng.

- Lập kế hoạch, bố trí nhân sự và các nguồn lực khác để thực hiện hợp đồng. Thông báo danh sách nhân sự triển khai cho Cảng vụ HKMT và phải được đơn vị chấp thuận. Nhân sự bên cung cấp dịch vụ phải ký cam kết không tiết lộ thông tin quan trọng của Cảng vụ HKMT.

- Đối với sản phẩm phần mềm: cung cấp mã nguồn phần mềm, thực hiện kiểm tra đánh giá an toàn thông tin, an ninh mạng, kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng.

- Phối hợp với Cảng vụ HKMT triển khai xây dựng hồ sơ đề xuất cấp độ ATTT đối với các HTTT mà đơn vị cho thuê hoặc cung cấp dịch vụ vận hành quản trị hệ thống đảm bảo đúng quy định tại Nghị định 85/2016/NĐ-CP ngày 01/7/2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ.

- Chịu trách nhiệm chủ động thực hiện giám sát an toàn thông tin, an ninh mạng đối với các hệ thống thông tin do mình quản lý theo quy định hiện hành.

3. Trách nhiệm của bộ phận quản trị HTTT, hệ thống mạng nội bộ tại Cảng vụ HKMT

- Mạng và đường truyền được áp dụng các chế độ bảo mật cần thiết, chống xâm nhập bất hợp pháp. Bộ phận quản trị mạng có trách nhiệm thường xuyên theo dõi, kiểm tra phát hiện kịp thời các hoạt động xâm nhập và có biện pháp xử lý kịp thời.

- Mạng nội bộ của Cảng vụ HKMT phải được trang bị hệ thống kỹ thuật firewall để 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. Ngăn chặn các trang mạng xã hội và các trang thông tin xấu độc có nguy cơ ảnh hưởng tới an toàn, an ninh thông tin mạng.

- Toàn bộ hệ thống máy tính thuộc mạng nội bộ của của đơn vị được đặt tên theo 1 nguyên tắc để dễ quản lý và kiểm soát, phải cài đặt phần mềm diệt virus có bản quyền. Bộ phận quản trị thường xuyên cập nhật các phiên bản mới, các bản vá lỗi của phần mềm chống virus để bảo đảm chương trình quét virus của các đơn vị và cá nhân trên các máy tính luôn được cập nhật mới nhất, thiết lập chế độ quét thường xuyên ít nhất là hàng tuần nhằm giảm thiểu tối đa tác hại của việc lây lan, tấn công của các loại virus, các loại mã nguồn độc hại và ngăn chặn kịp thời sự bùng nổ virus trong mạng nội bộ.

- Quản lý, vận hành, nâng cấp, bảo trì, sửa chữa và giám sát hệ thống mạng nội bộ; phát hiện các hành vi sử dụng mạng không hợp lệ; xử lý các lỗi kỹ thuật; ngăn ngừa các sự cố trên mạng để đảm bảo tính an toàn, tính tin cậy và đảm bảo sự vận hành thông suốt hệ thống mạng nội bộ.

- Lọc bỏ, chặn truy cập hoặc hạn chế truy cập các trang tin, ứng dụng có nghi ngờ chứa mã độc hoặc các nội dung không phù hợp phục vụ công việc.

- Phối hợp với các đơn vị có thẩm quyền như : Bộ Công an, Ban Cơ yếu chính phủ, Trung tâm ứng cứu khẩn cấp máy tính Việt Nam (VN-CERT), Trung tâm CNTT_Bộ GTVT và các đơn vị khác có liên quan để thường xuyên theo dõi và phối hợp ngăn ngừa nguy cơ tấn công mạng đảm bảo an toàn thông tin.

- Thường xuyên nghiên cứu, cập nhật các kiến thức về an toàn thông tin, có biện pháp phòng tránh các nguy cơ tiềm ẩn có thể gây mất thông tin khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ.

- Kịp thời thông báo cho các đơn vị, người sử dụng biết khi tạm dừng để nâng cấp, bảo trì định kỳ, khắc phục sự cố của từng dịch vụ mạng hoặc hệ thống mạng máy tính nội bộ.

4. Trách nhiệm của người sử dụng, khai thác dữ liệu trên HTTT và mạng nội bộ

- Nghiêm chỉnh thực hiện các quy chế quản lý, sử dụng các HTTT (Website, PO, Mail Online, TPublic…) và quy định về bảo đảm an toàn thông tin, an ninh mạng của Cảng vụ HKMT cũng như các quy định khác của pháp luật về nội dung này.

- Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo kịp thời cho bộ phận quản trị để kịp thời ngăn chặn và xử lý. Nâng cao ý thức

cảnh giác và trách nhiệm về an toàn thông tin, an ninh mạng.

- Không sử dụng mạng xã hội như: Google Plus+, MySpace, LinkedIn, X, Facebook, Zalo,..., và blog cá nhân để đăng tải, phát tán, truyền tải lại những nội dung phản động, tuyên truyền, xuyên tạc; không được truy cập vào các liên kết (link) không rõ ràng; không sử dụng địa chỉ thư điện tử công vụ vào mục đích cá nhân như: đăng ký tài khoản mạng xã hội, đăng ký mua sắm qua mạng...;

- Không sử dụng các hộp thư điện tử miễn phí Gmail, Yahoo,... trong hoạt động công vụ nhằm bảo đảm bảo mật, an toàn thông tin trên môi trường mạng. 100% viên chức thực hiện nhiệm vụ phải sử dụng hệ thống mail công vụ của đơn vị.

- Người sử dụng mạng nội bộ phải thường xuyên kiểm tra và diệt virus trên máy tính và các thiết bị ngoại vi gắn với máy tính mình đang sử dụng, trước khi gửi và sau khi nhận file dữ liệu. Không tự ý ngừng hoặc gỡ phần mềm diệt virus ra khỏi máy tính.

- Người sử dụng mạng nội bộ phải đặt chế độ bảo vệ màn hình và mật khẩu đăng nhập máy tính để đảm bảo an toàn cho dữ liệu cá nhân, khi không làm việc với máy tính trong thời gian dài phải thoát khỏi phiên làm việc và tắt máy. Mật khẩu tài khoản của cá nhân yêu cầu đặt mật khẩu phức tạp với độ an toàn cao để truy cập mạng, không được chuyển cho người khác sử dụng (Theo mục 3 điều 6 quy định này).

- Không được lợi dụng việc sử dụng HTTT và mạng nội bộ nhằm mục đích: Chống lại Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội; kích động bạo lực, đồi trụy, tệ nạn xã hội, mê tín dị đoan; phá hoại thuần phong mỹ tục của dân tộc; Không được truy cập hoặc tải các trang website có nội dung đồi trụy, phản động, các chương trình không rõ nguồn gốc, các thông tin quảng cáo.

CHƯƠNG IV
QUẢN LÝ SỰ CỐ AN TOÀN THÔNG TIN MẠNG

Điều 11. Phân nhóm sự cố an toàn thông tin mạng

1. Sự cố an toàn thông tin mạng nghiêm trọng là sự cố đáp ứng đồng thời các tiêu chí sau:

a. Hệ thống thông tin bị sự cố là hệ thống thông tin của đơn vị do các công ty dịch vụ làm quản trị máy chủ: Dữ liệu quan trọng của hệ thống không bảo đảm tính toàn vẹn và không có khả năng khôi phục được; Hệ thống bị mất quyền điều khiển; Sự cố có khả năng xảy ra trên diện rộng hoặc gây ra các ảnh hưởng dây chuyền, làm tổn hại cho các HTTT; ...

b. Chủ quản hệ thống thông tin không đủ khả năng tự kiểm soát, xử lý sự cố.

2. Sự cố an toàn thông tin mạng nội bộ thường gặp:

a. Sự cố do bị tấn công mạng;

b. Sự cố do lỗi hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật hoặc do lỗi đường truyền, hosting,…;

c. Sự cố do lỗi của người quản trị, vận hành hệ thống, ...;

Điều 12. Quy trình ứng cứu sự cố an toàn thông tin mạng

Bước 1: Thông báo sự cố

Cán bộ, viên chức, người lao động tại các phòng, các đại diện khi gặp sự cố trong quá trình sử dụng máy tính có kết nối mạng thực hiện thông báo ngay cho bộ phận đầu mối là phòng TCHC hoặc bộ phận CNTT tại đơn vị.

Bước 2: Tiếp nhận sự cố

Bộ phận CNTT tiếp nhận thông tin về sự cố qua các phương thức: điện thoại, trực tiếp, …

Bước 3: Xác minh/xác nhận sự cố

Bộ phận CNTT triển khai tiến hành Xác minh/xác nhận sự cố bao gồm các thông tin như sau:

- Tình trạng (Sự cố sẽ xảy ra; Sự cố đang xảy ra; Sự cố đã xảy ra);
- Mức độ (Sự cố nghiêm trọng; Sự cố bình thường);
- Phạm vi (Sự cố diện rộng; Sự cố mạng máy tính; Sự cố một máy tính);
- Và địa điểm xảy ra sự cố.

Bước 4: Phân loại sự cố

Bộ phận CNTT có trách nhiệm phân loại sự cố:

- Sự cố do lỗi hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật hoặc do lỗi đường truyền, hosting,…;
- Sự cố do lỗi của người quản trị, vận hành hệ thống;
- Sự cố do bị tấn công mạng nhưng trên phạm vi 01 máy tính, có thể khắc phục.
- Sự cố về tấn công phát tán mã độc (malware);
- Sự cố về tấn công từ chối dịch vụ (DoS/DDoS);
- Sự cố có yếu tố nước ngoài (hợp tác quốc tế);
- Sự cố tấn công khác.

Bước 5: Báo cáo lãnh đạo, xin ý kiến chỉ đạo

Ngay sau khi phân loại được sự cố, bộ phận CNTT có trách nhiệm báo cáo Lãnh đạo đơn vị để xem xét loại sự cố và tuỳ theo đối tượng sẽ tiến hành xử lý.

- Trường hợp sự cố được phân loại thông thường thì Bộ phận CNTT báo cho các bên liên quan để tiếp tục triển khai theo phương án ứng cứu sự cố an toàn thông tin mạng thông thường theo quy trình ứng cứu sự cố thông thường của Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017; báo cáo sự cố đến Đội ứng cứu sự cố an toàn thông tin mạng Bộ GTVT
- Trường hợp sự cố được phân loại nghiêm trọng thì gửi báo cáo sự cố đến Đội ứng cứu sự cố an toàn thông tin mạng Bộ GTVT về sự cố nghiêm trọng để có phương án ứng cứu; và tổ chức ứng cứu, xử lý sự cố:

Bước 6: Phối hợp với Đội ứng cứu sự cố an toàn thông tin mạng Bộ GTVT:

Thu thập thông tin phục vụ phân tích sự cố; Phân tích sự cố; Xử lý sự cố; Khôi phục, kiểm tra, báo cáo, tổng kết, đánh gía.

Tuân thủ các quy định pháp luật về điều phối, ứng cứu sự cố an toàn thông tin (ATTT) mạng.

Phối hợp chặt chẽ, chính xác, đồng bộ và hiệu quả giữa các cơ quan, đơn vị, ứng cứu sự cố trước hết phải được thực hiện, xử lý bằng lực lượng tại chỗ và trách nhiệm chính của đơn vị.

Đầu tư trang thiết bị bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố: Căn cứ điều kiện, tình hình thực tế tại đơn vị từ đó chủ động trang bị thiết bị, công cụ, phương tiện cần thiết để phục vụ ứng phó sự cố an toàn thông tin mạng; chuẩn bị các điều kiện bảo đảm, sẵn sàng đối phó, ứng cứu, khắc phục khi sự cố xảy ra

Bảo đảm bí mật thông tin khi tham gia, thực hiện các hoạt động ứng cứu sự cố.

CHƯƠNG V
TỔ CHỨC THỰC HIỆN

Điều 13. Tổ chức thực hiện

1. Căn cứ Quy định này, trưởng các phòng chuyên môn có trách nhiệm tổ chức triển khai thực hiện Quy định này trong phạm vi quản lý của mình.

2. Viên chức và người lao động tại các phòng chuyên môn có trách nhiệm thực hiện nghiêm túc Quy định này.

3. Các phòng, các đại diện thường xuyên kiểm tra việc thực hiện Quy định này tại đơn vị, coi đây là nhiệm vụ trọng tâm của đơn vị; chịu trách nhiệm trước pháp luật và Lãnh đạo Cảng vụ HKMT về các vi phạm, thất thoát thông tin, dữ liệu mật thuộc phạm vi quản lý của đơn vị do không tổ chức, chỉ đạo, kiểm tra cán bộ của đơn vị thực hiện đúng quy định.

4. Giao Phòng Tổ chức - Hành chính có trách nhiệm theo dõi, đôn đốc, kiểm tra, đánh giá việc thực hiện Quy định; đồng thời định kỳ báo cáo kết quả việc thực hiện cho cấp có thẩm quyền **trước ngày 30/11** hàng năm; thực hiện các báo cáo đột xuất theo sự cố an toàn thông tin và yêu cầu của cấp trên.

5. Trong quá trình thực hiện, nếu có vấn đề phát sinh hoặc khó khăn, vướng mắc cần phản ánh kịp thời về Phòng Tổ chức - Hành chính để tổng hợp báo cáo Giám đốc xem xét quyết định điều chỉnh, bổ sung cho phù hợp./.