BỘ TÀI CHÍNH **TỔNG CỤC HẢI QUAN**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 2926/QĐ-TCHQ	*Hà Nội, ngày 06 tháng 10 năm 2014*

QUYẾT ĐỊNH
Về việc ban hành Quy chế bảo đảm an ninh, an toàn Hệ thống Công nghệ thông tin Hải quan

TỔNG CỤC TRƯỞNG TỔNG CỤC HẢI QUAN

Căn cứ Luật Hải quan số 29/2001/QH10 ngày 29/06/2001; Luật số 42/2005/QH11 ngày 14/6/2005 sửa đổi, bổ sung một số điều của Luật Hải quan;

Căn cứ Luật giao dịch điện tử số 51/2005/QH11 ngày 29/11/2005;

Căn cứ Luật Công nghệ thông tin số 67/2006/QH11 ngày 29/06/2006;

Căn cứ Nghị định 174/2013/NĐ-CP ngày 13/11/2013 của Chính phủ quy định xử phạt vi phạm hành chính trong lĩnh vực Bưu chính, viễn thông, công nghệ thông tin và tần số vô tuyến điện;

Căn cứ Nghị định 64/2007/NĐ-CP ngày 10/04/2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

Căn cứ Quyết định số 02/2010/QĐ-TTg ngày 15 tháng 01 năm 2010 của Thủ tướng Chính phủ quy định về chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Tổng cục Hải quan trực thuộc Bộ Tài chính;

Xét đề nghị của Cục trưởng Cục Công nghệ Thông tin và Thống kê Hải quan,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này "Quy chế bảo đảm an ninh, an toàn Hệ thống công nghệ thông tin Hải quan".

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

Điều 3. Cục trưởng Cục Công nghệ Thông tin và Thống kê hải quan, Thủ trưởng các đơn vị thuộc, trực thuộc Tổng cục Hải quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như điều 3;
- Bộ Tài chính (để b/c);
- Lưu: VT, CNTT (5b).

KT. TỔNG CỤC TRƯỞNG
PHÓ TỔNG CỤC TRƯỞNG

Nguyễn Công Bình

BỘ TÀI CHÍNH
TỔNG CỤC HẢI QUAN

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

QUY CHẾ
BẢO ĐẢM AN NINH, AN TOÀN HỆ THỐNG CÔNG NGHỆ THÔNG TIN HẢI QUAN

(Ban hành kèm theo Quyết định số: 2926 /QĐ-TCHQ ngày 06 tháng 10 năm 2014 của Tổng cục trưởng Tổng cục Hải quan)

CHƯƠNG I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi áp dụng

Trong toàn bộ quá trình xây dựng, phát triển, quản lý, vận hành, khai thác, sử dụng Hệ thống công nghệ thông tin hải quan.

Điều 2. Đối tượng áp dụng

1. Các đơn vị thuộc, trực thuộc Tổng cục Hải quan.

2. Cán bộ, công chức, viên chức, người lao động trong ngành Hải quan.

3. Đối tác khi đến làm việc tại cơ quan hải quan.

Điều 3. Giải thích thuật ngữ, từ viết tắt

Trong Quy chế này, các từ ngữ dưới đây được hiểu như sau:

CNTT: Công nghệ thông tin.

TCHQ: Tổng cục Hải quan.

ANTT: An ninh thông tin.

Log: Ghi nhật ký.

ID: (Identification number) Tài khoản.

DC: Trung tâm dữ liệu (Data Center - DC) thuộc TCHQ.

DR: Trung tâm dự phòng (Disaster Recovery - DR) thuộc TCHQ.

TTDL&CNTT: Trung tâm dữ liệu và Công nghệ thông tin.

TTQLVH-HTCNTT: Trung tâm quản lý, vận hành hệ thống Công nghệ thông tin hải quan.

Cổng TTĐT Hải quan: Cổng thông tin điện tử Hải quan.

Tài sản CNTT: Bao gồm các trang thiết bị CNTT, các phần mềm thương mại, phần mềm ứng dụng.

Phương tiện xử lý thông tin: Hệ thống, dịch vụ hay cơ sở hạ tầng thông tin, hoặc các vị trí vật lý để đặt chúng.

An toàn thông tin: Sự duy trì tính bí mật, tính toàn vẹn và tính sẵn sàng; ngoài ra còn có thể bao hàm một số tính chất khác như tính xác thực; giải trình trách nhiệm, không thể chối bỏ và tin cậy.

Rủi ro: Sự kết hợp giữa khả năng xảy ra một sự kiện và hậu quả.

Đối tác: Tổ chức hay cá nhân (kể cả bên độc lập với tổ chức, cá nhân) tham gia các việc triển khai hệ thống, mạng, trang thiết bị CNTT; bảo đảm ANTT; nghiên cứu phát triển, kiểm thử, triển khai ứng dụng thuộc Hệ thống CNTT Hải quan.

Hệ thống Công nghệ thông tin hải quan: bao gồm hệ thống mạng, phần cứng máy tính và các thiết bị ngoại vi; hệ thống bảo đảm an ninh mạng, an toàn thông tin; phần mềm quản trị hệ thống, phần mềm ứng dụng triển khai tập trung, phân tán, phần mềm quản trị cơ sở dữ liệu triển khai tại TCHQ, Cục Hải quan các tỉnh, thành phố; các trang/cổng Thông tin điện tử trong ngành Hải quan.

Hệ thống mạng: bao gồm mạng cục bộ tại các đơn vị thuộc, trực thuộc TCHQ, mạng diện rộng ngành Hải quan.

Hệ thống an ninh thông tin: bao gồm phần cứng (máy tính và các thiết bị Firewall), phần mềm quản lý an ninh; các chính sách bảo đảm an ninh, an toàn thông tin.

Phần mềm: bao gồm phần mềm thương mại và phần mềm ứng dụng

Phần mềm ứng dụng: bao gồm phần mềm ứng dụng xử lý dữ liệu tập trung, phần mềm ứng dụng xử lý dữ liệu phân tán.

Phần mềm ứng dụng xử lý dữ liệu tập trung: là Hệ thống chương trình ứng dụng xử lý dữ liệu tập trung triển khai tại DC, DR, TTDL&CNTT (VNACCS/VCIS và các ứng dụng liên quan; Hệ thống thông quan một cửa quốc gia v.v..)

Phần mềm ứng dụng xử lý phân tán: là Hệ thống chương trình ứng dụng được xử lý dữ liệu phân tán cài đặt tại DC, DR; phòng máy chủ thuộc TTDL&CNTT, văn phòng Cục, Chi cục Hải quan.

Dữ liệu điện tử hải quan: là dữ liệu thu thập từ các Phần mềm ứng dụng xử lý dữ liệu tập trung, phân tán; các nguồn dữ liệu điện tử khác khác theo quy định (VD: văn bản quét trên mạng).

Phần mềm thương mại: là phần mềm đóng gói, triển khai trong các hệ thống CNTT như Windows Server; windows 20xx; SQL Server; Oracle; Virus v.v...

Người dùng: bao gồm quản trị viên, người sử dụng chương trình (gọi chung là người dùng).

Tài khoản người dùng: gồm tên truy cập và mật khẩu dùng để truy cập vào các chương trình trong Hệ thống CNTT Hải quan.

Mật khẩu đặc quyền: Mật khẩu duy nhất có đặc quyền cao (gọi tắt là mật khẩu đặc quyền) là mật khẩu của các tài khoản trọng yếu có quyền cao nhất đối với Hệ thống công nghệ thông tin Hải quan, như quyền cài đặt, cấu hình lại hệ thống, quyền tạo ra các tài khoản khác trong hệ thống, quyền khôi phục lại dữ liệu hoặc bản thân hệ thống từ các bản sao lưu.

Mật khẩu quản trị: Là các mật khẩu của tài khoản dùng để quản trị Hệ thống CNTT Hải quan (chỉ có một số quyền nhất định).

Mật khẩu người dùng: Mật khẩu của tài khoản người sử dụng khi đăng nhập Hệ thống Công nghệ thông tin Hải quan.

Xác thực đa nhân tố: Xác thực đa nhân tố dựa trên những thông tin mà người dùng biết (số PIN, mật khẩu) cùng với những gì mà người dùng có (SmartCard, USB, Token, Grid Card...) để chứng minh danh tính.

RAID (Redundant Arrays of Independent Disks): là hình thức ghép nhiều ổ đĩa cứng vật lý thành một hệ thống ổ đĩa cứng có chức năng gia tăng tốc độ đọc/ghi dữ liệu hoặc nhằm tăng thêm sự an toàn của dữ liệu chứa trên hệ thống đĩa hoặc kết hợp cả hai yếu tố trên.

Nhận dạng sinh trắc học: tức là sử dụng các đặc điểm hành vi và sinh học như dấu vân tay, dáng đi và thậm chí cả hình dạng tai để xác nhận danh tính.

Điều 4. Trách nhiệm bảo đảm an ninh, an toàn Hệ thống CNTT Hải quan của các đơn vị

1. Trách nhiệm quản lý, bảo đảm ANTT của Cục CNTT&Thống kê hải quan

a) Hệ thống mạng và trang thiết bị CNTT

- Mạng diện rộng (WAN) ngành Hải quan;

- Hệ thống mạng nội bộ (LAN) và trang thiết bị CNTT triển khai tại DC, DR và cơ quan TCHQ;

- Hệ thống bảo đảm an ninh, an toàn cho Hệ thống CNTT Hải quan tại các DC, DR;

- Máy tính và thiết bị CNTT tại Cục CNTT&Thống kê hải quan.

b) Phần mềm thương mại: Triển khai tại DC, DR và Hệ thống máy tính của Cục CNTT&Thống kê hải quan.

c) Phần mềm ứng dụng:

- Phần mềm ứng dụng xử lý dữ liệu tập trung, phân tán triển khai tại DC, DR;

- Cổng Thông tin điện tử Hải quan.

2. Trách nhiệm quản lý, bảo đảm ANTT Cục Hải quan các tỉnh, thành phố

a) Hệ thống mạng và trang thiết bị CNTT

- Mạng diện rộng (WAN) từ Cục Hải quan các tỉnh thành phố tới các Chi cục Hải quan;

- Hệ thống mạng LAN, máy tính triển khai tại các TTDL&CNTT, Phòng máy chủ, văn phòng làm việc tại Cục, Chi cục Hải quan;

- Hệ thống bảo đảm an ninh, an toàn thông tin tại TTDL&CNTT, các Phòng máy chủ thuộc Cục;

- Máy tính và trang bị CNTT tại Cục Hải quan các tỉnh, thành phố, Chi cục Hải quan trực thuộc.

b) Phần mềm thương mại:

- Trang bị tại TTDL&CNTT, Phòng máy chủ, các máy tính thuộc Cục Hải quan các tỉnh, thành phố.

c) Phần mềm ứng dụng

- Phần mềm ứng dụng xử lý dữ liệu tập trung, phân tán triển khai tại TTDL&CNTT, Phòng Máy chủ thuộc Cục, Chi cục Hải quan;

- Các phần mềm ứng dụng khác do Cục Hải quan tỉnh, thành phố phát triển, triển khai tại đơn vị;

- Hoạt động của trang/cổng thông tin điện tử hải quan do Cục Hải quan tỉnh, thành phố quản lý.

3. Trách nhiệm quản lý, bảo đảm ANTT của các đơn vị thuộc cơ quan TCHQ

a) Hệ thống mạng và trang thiết bị CNTT trang bị tại đơn vị.

b) Các phần mềm thương mại triển khai trên các máy tính do đơn vị quản lý.

c) Phần mềm ứng dụng

- Phần mềm ứng dụng xử lý dữ liệu tập trung, phân tán triển khai trên các máy tính do đơn vị quản lý, vận hành.

- Hoạt động của trang/cổng Thông tin điện tử do đơn vị quản lý.

Điều 5. Tổ chức đảm bảo an ninh, an toàn cho Hệ thống CNTT Hải quan

1. Quy định về tổ chức

a) Trách nhiệm của Lãnh đạo về đảm bảo an ninh, an toàn

Lãnh đạo Hải quan các cấp phải nhận thức rõ tầm quan trọng về bảo đảm an ninh, an toàn cho Hệ thống CNTT Hải quan; tổ chức triển khai, giám sát kết quả thực hiện các quy định về đảm bảo an ninh, an toàn cho Hệ thống CNTT tại đơn vị mình.

b) Phối hợp về đảm bảo an ninh, an toàn

- Các đơn vị thuộc, trực thuộc TCHQ có trách nhiệm phối hợp với Cục CNTT & Thống kê hải quan thực hiện các quy định về đảm bảo an ninh, an toàn cho Hệ thống thông tin Hải quan.

- Đối tác khi thực hiện các công việc liên quan đến Hệ thống CNTT Hải quan phải thực hiện quy định về bảo đảm an ninh, an toàn thông tin.

c) Liên lạc với các cơ quan/tổ chức có thẩm quyền

- Cục CNTT & Thống kê hải quan là đơn vị đầu mối của Tổng cục Hải quan làm việc với Bộ Tài chính, Bộ Thông tin truyền thông, các cơ quan, tổ chức có thẩm quyền; các nhóm chuyên gia, hiệp hội an toàn an ninh thông tin để bảo đảm an ninh, an toàn Hệ thống CNTT Hải quan.

- Các TTDL & CNTT, các đơn vị phụ trách CNTT (đối với các Cục hải quan không có TTDL & CNTT) chủ trì, đầu mối trong phối hợp với Cục CNTT & Thống kê hải quan và các đơn vị quản lý chuyên ngành tại địa phương về đảm bảo an ninh, an toàn cho Hệ thống CNTT Hải quan.

2. Quy định về bảo đảm an ninh, an toàn nguồn nhân lực CNTT

Các đơn vị thuộc, trực thuộc TCHQ thực hiện:

a) Xác định nhiệm vụ vị trí tuyển dụng, phân công thực hiện công tác bảo đảm an ninh, an toàn Hệ thống CNTT Hải quan.

b) Kiểm tra lý lịch, xem xét đánh giá nghiêm ngặt tư cách đạo đức, trình độ chuyên môn khi tuyển dụng, phân công cán bộ, công chức, viên chức làm việc tại các vị trí trọng yếu của hệ thống CNTT như quản trị hệ thống, quản trị hệ thống an ninh thông tin, quản trị ứng dụng và cơ sở dữ liệu.

c) Quyết định phân công hoặc hợp đồng tuyển dụng (nếu có) phải quy định các điều khoản về trách nhiệm đảm bảo an ninh, an toàn Hệ thống CNTT Hải quan của người được giao nhiệm vụ, làm việc trong Hệ thống CNTT Hải quan.

3. Quản lý cán bộ, công chức, viên chức

Đơn vị hải quan quản lý trực tiếp cán bộ, công chức, viên chức chấm dứt hoặc thay đổi công việc phải:

a) Xác định rõ trách nhiệm của cán bộ, công chức, viên chức và các bên liên quan trong thời gian làm việc trong Hệ thống CNTT Hải quan.

b) Lập biên bản bàn giao tài sản CNTT với cán bộ, công chức, viên chức.

c) Thu hồi hoặc thay đổi quyền truy cập vào Hệ thống CNTT Hải quan của cán bộ, công chức, viên chức cho phù hợp với công việc được thay đổi.

Điều 6. Đảm bảo an ninh, an toàn khi có sự tham gia của đối tác

1. Quy định chung

- Trước khi đến làm việc, đối tác phải ký với cơ quan hải quan chủ trì thỏa thuận, thực hiện bảo đảm an ninh, an toàn Hệ thống CNTT Hải quan;

- Đối tác chỉ làm việc tại khu vực mạng riêng cho đối tác; không được tùy tiện làm việc ở những nơi ngoài quy định khi chưa được phép;

- Được truy cập vào phần mã nguồn, dữ liệu mà hai bên đã thỏa thuận.

2. Quy định thủ tục với người của đối tác đến làm việc

- Xuất trình giấy ra vào với đơn vị chủ trì tại bàn đón tiếp tòa nhà (chứng minh thư hoặc hộ chiếu, giấy liên hệ công tác), và chỉ vào cơ quan khi được cấp thẻ khách hoặc được phép của Bộ phận đón tiếp;

- Khi vào, ra phải được phép, có sự giám sát, hướng dẫn của cán bộ trực tại DC, DR;

- Khi ra vào TTDL&CNTT hoặc các phòng máy chủ tại Cục Hải quan các tỉnh, thành phố phải được phép, và có sự giám sát, hướng dẫn của cán bộ thuộc đơn vị chủ quản.

3. Quy định quản lý, bảo đảm an ninh chống lại phần mềm độc hại

- Người của đối tác khi đến làm việc tại cơ quan hải quan không được sử dụng các thiết bị thông minh (SmartPhone) để truy cập vào máy tính trong mạng nội bộ của cơ quan hải quan;

- Không được tự ý cài đặt thêm bất cứ phần mềm nào vào máy tính của cơ quan hải quan;

- Không được truy cập vào thư điện tử của cơ quan hải quan dưới mọi hình thức, khi không được phép.

4. Quy định kiểm tra, giám sát của cơ quan hải quan với đối tác

Cục CNTT&Thống kê hải quan, TTDL&CNTT, đơn vị quản lý bộ phận CNTT (Cục Hải quan chưa có TTDL&CNTT):

- Tổ chức hướng dẫn các quy định cho đối tác trước khi tham gia vào Hệ thống CNTT Hải quan;

- Quản lý, giám sát đối tác khi làm việc liên quan tới Hệ thống CNTT Hải quan;

- Thường xuyên kiểm tra, giám sát phát hiện các ảnh hưởng có thể gây ra đối với Hệ thống CNTT Hải quan.

CHƯƠNG II

ĐẢM BẢO AN NINH, AN TOÀN TRONG THIẾT KẾ, XÂY DỰNG, TRIỂN KHAI HỆ THỐNG CNTT HẢI QUAN

MỤC 1

TRANG THIẾT BỊ CÔNG NGHỆ THÔNG TIN

Điều 7. Đảm bảo an ninh, an toàn phòng máy chủ

1. Phòng máy chủ: phòng máy chủ tại DC, DR, TTDL&CNTT, Cục Hải quan các tỉnh, thành phố (chưa có TTDL&CNTT), Chi cục Hải quan phải được bố trí thành phòng riêng, với các thiết bị CNTT đang hoạt động trong các Hệ thống CNTT Hải quan.

2. Môi trường hoạt động của Phòng máy chủ

a) Môi trường khô ráo, sạch sẽ, không dột, không thấm nước, các trang thiết bị lắp đặt trên sàn kỹ thuật, không bị ánh nắng chiếu rọi trực tiếp. Độ ẩm, nhiệt độ đạt tiêu chuẩn quy định cho các thiết bị tin học.

b) Diện tích phòng máy chủ tại Cục Hải quan phải đảm bảo đủ diện tích, chiều cao để bố trí đủ các trang thiết bị CNTT và hạ tầng kỹ thuật chung; có các biện pháp kỹ thuật, hành chính ngăn chặn việc tiếp cận trái phép các trang thiết bị, đường truyền mạng trong và ngoài phòng máy chủ.

3. Trang bị các thiết bị bảo đảm an ninh, an toàn

a) Hệ thống phòng cháy, chữa cháy

- Phòng máy chủ được bố trí hệ thống phòng cháy, chữa cháy chuyên dùng cho phòng máy tính.

- Bố trí các thiết bị dập cháy như bình bọt, bình CO2, v.v..

b) Hệ thống điện

- Phòng máy chủ được bố trí hệ thống điện đủ công suất hoạt động cho các thiết bị lắp đặt trong phòng.

- Có hai đường dẫn diện khác nhau để phòng rủi ro.

- Trang bị hệ thống phát điện, nhiên liệu dự phòng khi mất điện.

c) Hệ thống lưu điện (UPS)

- Thiết bị trong phòng máy chủ được bố trí hệ thống lưu điện tập trung hoặc cho từng thiết bị, đủ công suất hoạt động.

- Kiểm tra thiết bị lưu điện phải bảo đảm hoạt động khi có sự cố mất điện.

d) Hệ thống tiếp đất

- Phòng máy chủ được bố trí hệ thống tiếp đất theo tiêu chuẩn an toàn cho hệ thống máy tính.

- Kiểm tra thường xuyên, bảo đảm hoạt động của hệ thống tiếp đất.

đ) Hệ thống chống sét lan truyền

- Phòng máy chủ được bố trí hệ thống chống sét bao gồm: chống sét đánh thẳng, sét đánh lan truyền qua đường cấp điện nguồn, điện thoại, đường mạng.

- Kiểm tra, bảo đảm hệ thống chống sét hoạt động liên tục.

e) Hệ thống điều hoà

- Phòng máy chủ được bố trí hệ thống điều hòa làm mát, bảo đảm nhiệt độ và độ ẩm cho thiết bị theo tiêu chuẩn của nhà sản xuất quy định.

- Có hệ thống điều hòa dự phòng cho các phòng máy chủ, bảo đảm hệ thống điều hòa phải hoạt động liên tục 24/24h các ngày, đủ công suất.

f) Hệ thống camera giám sát

- Phòng máy chủ tại DC, DR, TTDL&CNTT có hệ thống Camera giám sát hoạt động liên tục 24/24h các ngày.

- Hệ thống Camera giám sát được kết nối với máy tính để lưu trữ dữ liệu và máy tính của bộ phận giám sát.

4. Hệ thống máy chủ trang/cổng thông tin điện tử

a) Hệ thống máy chủ của trang/cổng thông tin điện tử bố trí tối thiểu mô hình (2 lớp): máy chủ cài chương trình ứng dụng web độc lập với máy chủ quản trị dữ liệu; trong điều kiện cho phép có thể bố trí theo mô hình an ninh cao hơn (n lớp), có cân bằng tải cho các máy chủ ứng dụng web.

b) Máy chủ web đặt tại DC, TTDL&CNTT, phòng máy chủ của đơn vị, phải tuân thủ theo đúng thiết kế, đặt trong vùng mạng dành cho máy chủ web, có tường lửa bảo đảm an ninh, an toàn và thực hiện kiểm soát an ninh.

c) Máy chủ web đang thuê đặt bên ngoài, đơn vị quản lý trang/cổng thông tin điện tử phải có các thỏa thuận, điều khoản bảo đảm về an ninh, an toàn đối với nhà cung cấp dịch vụ như đặt tường lửa, kiểm soát truy cập trái phép v.v... .

Điều 8. Đảm bảo an ninh, an toàn trang thiết bị CNTT trong quá trình triển khai lắp đặt trước khi sử dụng

1. Kiểm tra trang thiết bị CNTT

a) Không có phần mềm đã cài đặt sẵn trong các thiết bị CNTT(máy chủ, máy trạm, trang thiết bị CNTT), trường hợp thiết bị CNTT đã có sẵn phần mềm, đơn vị quản lý trang thiết bị CNTT phải kiểm tra, nếu phát hiện phần mềm độc hại, phải thực hiện các biện pháp xử lý, để bảo đảm an ninh, an toàn tuyệt đối.

b) Thiết bị phải đúng nguồn gốc, xuất xứ thuộc Quyết định khi triển khai hợp đồng.

c) Lập biên bản quá trình kiểm tra, xử lý thiết bị CNTT.

2. Triển khai trang thiết bị CNTT

a) Triển khai trang thiết bị CNTT tới các vị trí trong bản thiết kế, hoặc kế hoạch trang bị thiết bị CNTT đã được phê duyệt của cấp thẩm quyền.

b) Thực hiện các biện pháp bảo đảm an ninh trong quá trình triển khai trang thiết bị CNTT như vận chuyển an toàn, không tiết lộ mục đích sử dụng của thiết bị cho những người không có thẩm quyền biết v.v.. .

c) Sau khi triển khai xong thiết bị, thực hiện kiểm thử, vận hành.

d) Thực hiện các thủ tục bàn giao trang thiết bị CNTT theo các quy định hiện hành.

MỤC 2
HỆ THỐNG MẠNG

Điều 9. Đảm bảo an ninh, an toàn cho hệ thống

1. Thiết kế mạng diện rộng

Thiết kế và vận hành mạng diện rộng theo Quy chế quản lý, vận hành và sử dụng hạ tầng truyền thông thống nhất ngành Tài chính ban hành tại Quyết định số 109/QĐ-BTC ngày 15/01/2009 của Bộ trưởng Bộ Tài chính và các văn bản sửa đổi, cập nhật quy chế này nếu có.

2. Phân vùng và thiết kế mạng nội bộ

a) Phân vùng mạng nội bộ

- Phân chia hệ thống mạng nội bộ thành các vùng mạng theo phạm vi truy cập, thực hiện kiểm soát truy cập giữa các vùng bằng tường lửa. Phân chia các vùng mạng tối thiểu như sau:

+ Vùng mạng cho truy cập từ Internet khu vực để dữ liệu trung gian (DMZ) truy cập internet áp dụng với các dịch vụ công hoặc ứng dụng cung cấp ra Internet đối với trang/cổng thông tin điện tử đặt tại đơn vị.

+ Vùng mạng truy cập Internet (trung chuyển các yêu cầu truy cập Internet từ người dùng hoặc máy chủ);

+ Vùng mạng máy chủ nội bộ;

+ Vùng mạng quản trị (các hoạt động quản trị hệ thống, quản trị ANTT phải được thực hiện thông qua vùng mạng này);

+ Vùng mạng người dùng, trong đó tách riêng vùng mạng cho kết nối có dây và không dây;

+ Vùng mạng riêng đối tác: áp dụng cho đối tác tới làm việc tại cơ quan hải quan theo các thỏa thuận, hợp đồng có các công việc liên quan đến các Hệ thống CNTT Hải quan.

- Vô hiệu hóa (tắt) tất cả các dịch vụ không sử dụng tại từng vùng mạng.

- Thực hiện các biện pháp bảo mật, tránh truy cập trực tiếp từ ngoài tới các địa chỉ mạng bên trong (Internet, hạ tầng truyền thông ngành Hải quan).

- Cài đặt các bản cập nhật, vá lỗi đúng hạn cho các tường lửa để khắc phục các điểm yếu an ninh nghiêm trọng; thực hiện chế độ bảo hành hoặc thiết bị dự phòng để đảm bảo sự hoạt động liên tục của tường lửa.

b) Thiết kế mạng nội bộ

- Khi thiết kế mạng nội bộ (LAN): Bảo đảm đáp ứng các hoạt động nghiệp vụ, năng lực hoạt động của hệ thống và khả năng dự phòng (bảo đảm nút mạng/người; giải thông; tiêu chuẩn về dây cáp, đầu nối mạng, tiêu chuẩn đi dây nối mạng, biện pháp chống nhiễu).

- Lãnh đạo đơn vị chủ trì quản lý Hệ thống CNTT Hải quan phê duyệt toàn bộ sơ đồ thiết kế.

c) Triển khai lắp đặt mạng nội bộ

- Triển khai lắp đặt mạng nội bộ phải đúng với sơ đồ thiết kế đã được cấp thẩm quyền phê duyệt; các trang thiết bị kỹ thuật mạng bảo đảm đúng xuất xứ nguồn gốc, tiêu chuẩn kỹ thuật và bảo đảm mỹ quan.

- Triển khai các biện pháp giám sát trong quá trình thi công lắp đặt mạng và thiết bị mạng;

- Thực hiện kiểm thử mạng sau khi hoàn thành lắp đặt bằng các giải pháp kỹ thuật khác nhau, bảo đảm mạng khi đi vào hoạt động đáp ứng các năng lực của hệ thống như thiết kế.

d) Triển khai các phần mềm thương mại

- Các phần mềm thương mại (VD: Windows Server, windows xx, v.v...) phải có bản quyền; thực hiện kiểm thử trước khi triển khai chính thức.

- Triển khai, cài đặt các phần mềm thương mại trên Hệ thống CNTT Hải quan và các phần mềm khác để bảo đảm môi trường triển khai ứng dụng nghiệp vụ, quản lý của cơ quan Hải quan.

- Triển khai cài đặt ngay các bản vá mới nhất của các phần mềm thương mại (bản vá của chính hãng cấp hoặc nguồn gốc cung cấp tin cậy), các phần mềm ngăn chặn mã độc hại và các phần mềm khác bảo đảm đủ môi trường triển khai ứng dụng nghiệp vụ, ứng dụng chuyên môn khác của ngành Hải quan.

MỤC 3
PHẦN MỀM ỨNG DỤNG

Điều 10. Quy định đảm bảo an ninh, an toàn trong thiết kế ứng dụng

1. Các tài liệu phân tích yêu cầu người sử dụng; tài liệu thiết kế hệ thống của phần mềm ứng dụng; tài liệu đào tạo, chuyển giao công nghệ và các tài liệu liên quan phải lưu trữ đầy đủ, an toàn.

2. Tài liệu thiết kế hệ thống của phần mềm ứng dụng chỉ được lưu trên các máy trạm an toàn (có cài hệ thống phát hiện phòng chống mã độc, không cho phép truy cập từ xa, cài đặt mật khẩu xác thực mạnh). Không lưu trữ tài liệu thiết kế hệ thống phần mềm ứng dụng trên các phương tiện lưu trữ thông tin có thể dịch chuyển, nếu lưu trữ tạm thời cần có biện pháp bảo mật và xóa ngay sau khi vậ¤;'n chuyển.

3. Tài liệu thiết kế hệ thống của phần mềm ứng dụng có sự tham gia của đối tác, phải có thỏa thuận về đảm bảo an ninh, an toàn cho tài liệu.

Điều 11. Quy định đảm bảo an ninh, an toàn trong xây dựng phần mềm ứng dụng

1. Xây dựng phần mềm ứng dụng

a) Phải có quy định bảo đảm an ninh, an toàn từ mã nguồn khi phát triển phần mềm.

b) Các công cụ phát triển, xây dựng phần mềm phải có bản quyền.

c) Khi xây dựng Phần mềm ứng dụng phải thực hiện đúng, đầy đủ các chức năng đã được mô tả trong nội dung yêu cầu nghiệp vụ - kỹ thuật.

d) Đối tác tham gia phát triển hệ thống thông tin phải ký cam kết bảo đảm an ninh, an toàn các giai đoạn trong quá trình xây dựng phần mềm ứng dụng.

2. Kiểm thử phần mềm ứng dụng

a) Phần mềm phát triển, kiểm thử phải chạy trên các hệ thống hoặc bộ vi xử lý máy tính khác nhau và nằm trong các thư mục, tên miền khác nhau với hệ thống vận hành chính thức.

b) Môi trường hệ thống kiểm thử cần được mô phỏng giống môi trường khai thác gần nhất đến mức có thể để thực hiện các biện pháp kiểm tra an ninh, an toàn.

c) Không được sao chép dữ liệu nhạy cảm vào môi trường hệ thống kiểm thử.

d) Tài khoản dùng khi truy cập để kiểm thử phần mềm khác tài khoản truy cập vào phần mềm triển khai chính thức.

Điều 12. Quy định đảm bảo an ninh, chuẩn bị triển khai ứng dụng

1. Cập nhật, kiểm tra dữ liệu chuẩn

a) Cục CNTT&Thống kê hải quan

- Thông báo tới các đơn vị nghiệp vụ cung cấp mới và bổ sung đủ, chính xác, đúng thời gian dữ liệu chuẩn cho từng phần mềm ứng dụng;

- Thực hiện nhập số liệu cho các tệp dữ liệu chuẩn, đôn đốc và phối hợp với các đơn vị nghiệp vụ trong việc nhập dữ liệu chuẩn (đã phân công cụ thể đối với từng phần mềm ứng dụng) bảo đảm đúng thời gian, chính xác và đầy đủ dữ liệu;

- Kiểm tra tính hợp lệ, đầy đủ, chính xác của dữ liệu chuẩn.

b) Các Cục, Vụ nghiệp vụ thuộc TCHQ:

- Chịu trách nhiệm cung cấp thông tin dữ liệu chuẩn của từng hệ thống (đã phân công cụ thể đối với từng phần mềm ứng dụng); dữ liệu bảo đảm chính xác, đủ và đúng thời gian quy định;

- Tham gia cập nhật dữ liệu chuẩn, kiểm tra dữ liệu chuẩn theo quy định.

2. Kiểm tra các tệp trong cơ sở dữ liệu

a) Kiểm tra ngẫu nhiên dữ liệu đầu vào hoặc sử dụng các hình thức kiểm tra khác nhau để kiểm tra tính hợp lệ, đủ và chính xác của dữ liệu đầu vào của ứng dụng;

b) Kiểm tra định kỳ nội dung các trường chính hoặc các tệp dữ liệu trong phần mềm ứng dụng, nhằm xác định tính toàn vẹn và hợp lệ của chúng.

c) Ghi nhật ký các hoạt động liên quan đến quá trình xử lý dữ liệu.

Điều 13. Quy định đảm bảo an ninh, an toàn trong triển khai phần mềm ứng dụng

1. Quy định chung

a) Trước khi triển khai chính thức, phải thực hiện quét và khắc phục lỗ hổng bảo mật phần mềm ứng dụng.

b) Chương trình đã triển khai chính thức định kỳ năm/lần kiểm tra, khắc phục lỗ hổng bảo mật của ứng dụng; đối với ứng dụng quan trọng sáu tháng/lần kiểm tra, khắc phục lỗ hổng bảo mật.

c) Lãnh đạo đơn vị chủ trì, thực hiện phê duyệt phần mềm ứng dụng được triển khai chính thức.

2. Quy định triển khai với Phần mềm ứng dụng nâng cấp

a) Trước khi triển khai chính thức, thực hiện sao chép (backup) lại toàn bộ các chương trình, ứng dụng và cơ sở dữ liệu của chương trình đang hoạt động.

b) Thực hiện biện pháp kiểm thử, bảo đảm toàn bộ chương trình, ứng dụng và dữ liệu đã sao chép, khi thực hiện khôi phục phải đảm bảo hoạt động bình thường.

c) Triển khai chính thức ứng dụng và cơ sở dữ liệu; kiểm tra hoạt động của ứng dụng và cơ sở dữ liệu sau khi triển khai chính thức, bảo đảm hoạt động tốt, đáp ứng các chức năng của chương trình.

d) Sau khi triển khai chính thức, chương trình ứng dụng và cơ sở dữ liệu không đảm bảo hoạt động, đáp ứng đủ các chức năng của chương trình, bộ phận

triển khai phải thực hiện khôi phục lại chương trình và cơ sở dữ liệu của hệ thống đã triển khai trước đây, để bảo đảm các hoạt động nghiệp vụ không bị gián đoạn.

3. Quy định với Phần mềm ứng dụng triển khai lần đầu

a) Cài đặt, cấu hình an ninh, an toàn đầy đủ hệ điều hành, phần mềm hệ thống, hệ quản trị cơ sở dữ liệu, và các phần mềm khác bảo đảm môi trường để triển khai ứng dụng.

b) Cài đặt các chương trình phòng, chống mã độc hại …

c) Cài đặt ứng dụng; cơ sở dữ liệu.

d) Kiểm tra hoạt động của chương trình ứng dụng và dữ liệu, bảo đảm hoạt động bình thường.

đ) Có đầy đủ tài liệu hướng dẫn sử dụng các chức năng Phần mềm ứng dụng triển khai lần đầu.

CHƯƠNG III
ĐẢM BẢO AN NINH, AN TOÀN TRONG VẬN HÀNH GIÁM SÁT HỆ THỐNG CÔNG NGHỆ THÔNG TIN HẢI QUAN

MỤC 1
TRANG THIẾT BỊ CÔNG NGHỆ THÔNG TIN

Điều 14. Đảm bảo an ninh, an toàn khi vận hành trang thiết bị CNTT

Cán bộ, công chức, viên chức thực hiện các quy định sau:

1. Quy định an ninh, an toàn khi sử dụng máy tính

a) Chỉ được sử dụng máy tính vào các hoạt động nghiệp vụ.

b) Không sử dụng máy tính để truy cập, tải về, lưu trữ, phát tán văn hóa phẩm đồi trụy hoặc những nội dung vi phạm pháp luật.

c) Kiểm tra nguồn điện trước khi bật máy tính cá nhân.

d) Không để chất lỏng, hóa chất, chất dễ cháy nổ ở gần và có thể gây nguy cơ hư hỏng đến máy tính cá nhân.

e) Không tự tiện thay đổi cấu hình, phần cứng của máy tính cá nhân.

f) Không tự tiện cài đặt, thay đổi, gỡ bỏ các ứng dụng, phần mềm, chương trình hiện có trên máy tính; không được tải về và cài đặt các phần mềm dò quét mật khẩu, tấn công và dò quét mạng.

g) Không sử dụng máy tính để truy cập, cố gắng truy cập tới các hệ thống không được phân quyền.

h) Không được cung cấp tài khoản sử dụng máy tính cho người khác.

i) Đặt và sử dụng mật khẩu theo "Quy định về quản lý mật khẩu".

j) Các dữ liệu xếp hạng mật hay tuyệt mật lưu trữ trên máy tính cá nhân phải tuân thủ quy định về quản lý tài liệu mật.

k) Khóa màn hình máy tính khi rời khỏi bàn làm việc.

l) Đăng xuất khỏi hệ thống, ứng dụng khi ngừng sử dụng.

m) Tắt máy sau mỗi buổi làm việc.

2. Quy định an ninh, an toàn khi sử dụng thiết bị di động: đĩa cứng rời, USB

a) Chỉ sử dụng ổ đĩa cứng rời, USB cho các hoạt động nghiệp vụ, quản lý khi được sự đồng ý của Lãnh đạo đơn vị.

b) Thực hiện các biện pháp bảo đảm an ninh, an toàn cho đĩa cứng rời và USB như khi sử dụng máy tính.

3. Thiết bị CNTT hoạt động bên ngoài trụ sở

a) Thiết bị và phương tiện xử lý thông tin khi mang ra ngoài trụ sở phải bảo đảm an toàn, tránh bị chú ý, trộm cắp, nghe trộm, trường hợp làm mất hoặc lộ thông tin trên thiết bị và phương tiện xử lý thông tin có chứa dữ liệu về hệ thống CNTT Hải quan, phải báo ngay cho lãnh đạo và đơn vị có thẩm quyền để có biện pháp khắc phục kịp thời.

b) Lãnh đạo đơn vị triển khai các biện pháp quản lý phù hợp, bảo đảm an ninh, an toàn với các thiết bị làm việc ngoài trụ sở hải quan. VD cài đặt các phần mềm phòng chống mã độc, chống nghe trộm, giám sát truy cập v.v...

Điều 15. Quy định an toàn cho thiết bị, thông tin di dời, hết hạn sử dụng, tái sử dụng

1. Quy định loại phương tiện xử lý thông tin di dời

a) Lãnh đạo đơn vị phê duyệt danh mục phương tiện sẽ loại khỏi cơ quan.

b) Phân công cán bộ, công chức, viên chức thực hiện chuyển các phương tiện di dời.

2. Loại bỏ thông tin trên phương tiện xử lý thông tin

a) Phương tiện lưu giữ thông tin khi hết hạn sử dụng được lưu giữ cẩn thận.

b) Thực hiện định danh phương tiện bị loại bỏ và thực hiện loại bỏ an toàn (không thể khôi phục được), ví dụ: đốt, cắt nhỏ, xóa dữ liệu.

c) Có thể tập trung toàn bộ thiết bị xử lý thông tin đã hết hạn sử dụng, thực hiện loại bỏ an toàn tập trung; (đốt, cán hỏng v.v...).

d) Nhật ký việc loại bỏ phương tiện nhằm duy trì truy vết.

3. Quy định an toàn khi tái sử dụng thiết bị xử lý thông tin

a) Thiết bị xử lý thông tin khi tái sử dụng: Tất cả các bộ phận thiết bị có chứa các phương tiện lưu trữ thông tin phải được kiểm tra kỹ, bảo đảm rằng các dữ liệu nhạy cảm và phần mềm có bản quyền phải được xóa bỏ hoặc ghi đè trước khi loại bỏ hoặc tái sử dụng thiết bị cho mục đích khác.

b) Các thiết bị hư hỏng lại chứa các dữ liệu nhạy cảm cần được đánh giá, xác định phương pháp loại bỏ.

MỤC 2
HỆ THỐNG MẠNG

Điều 16. Kiểm soát truy cập

1. Quản lý truy cập mạng

a) Chính sách truy cập mạng, Hệ thống CNTT Hải quan

- Cán bộ, công chức, viên chức được phép truy cập vào mạng, hệ thống CNTT Hải quan (từ trong hệ thống mạng) để tác nghiệp nghiệp vụ.

- Chỉ Quản trị viên hệ thống được lãnh đạo đơn vị phân công mới thực hiện truy cập từ xa (bên ngoài) vào Hệ thống CNTT Hải quan để tác nghiệp, xử lý kỹ thuật.

- Quản trị viên hệ thống: khi thực hiện truy cập từ bên ngoài vào Hệ thống CNTT Hải quan, phải thực hiện các biện pháp bảo đảm an ninh, an toàn cho các phương tiện xử lý thông tin (cài đặt các hệ thống giám sát, phòng chống mã độc, chống nghe trộm, chống lấy cắp tài khoản v.v...); các thông tin quan trọng khi truy cập từ ngoài vào Hệ thống CNTT Hải quan phải thực hiện các biện pháp mã hóa, bảo đảm an ninh, an toàn.

- Lãnh đạo đơn vị tổ chức cho cán bộ, công chức, viên chức thực hiện đăng ký và phê duyệt danh sách đề nghị cấp tài khoản truy cập mạng, thu hồi tài khoản với người thay đổi vị trí, không tiếp tục công việc.

b) Xác thực người dùng cho kết nối bên ngoài

- Lãnh đạo đơn vị phê duyệt danh sách cán bộ, công chức, viên chức được truy cập từ bên ngoài qua (VPN) để khai thác thông tin nghiệp vụ, quản lý trong mạng nội bộ hoặc đề nghị thu hồi tài khoản đối với cán bộ, công chức đã thay đổi vị trí công việc, không tham gia truy cập qua mạng ảo (VPN) để vào Hệ thống NetOffice; Hệ thống thông quan điện tử tập trung (có quản lý chuyển cửa khẩu) gửi về TCHQ (Cục CNTT&Thống kê hải quan) để cấp, hoặc thu hồi tài khoản truy cập.

- Cục CNTT&Thống kê hải quan: Kiểm tra, cấp tài khoản truy cập (quyền truy cập) từ xa; thường xuyên rà soát thu hồi quyền truy cập từ xa với cán bộ, công chức đã ngừng công việc, chuyển đổi vị trí công tác, không được giao nhiệm vụ truy cập lấy thông tin qua mạng ảo VPN.

c) Định danh thiết bị trong mạng

- Triển khai thiết bị giám sát, kiểm tra tình trạng hoạt động của mạng, các thiết bị đang kết nối trong hệ thống mạng.

- Thiết bị giám sát cần chỉ rõ địa chỉ mà thiết bị đang kết nối; địa chỉ bị ngắt kết nối, để giúp quá trình giám sát, xử lý kịp thời sự cố.

d) Chuẩn đoán, bảo vệ cấu hình mạng

Cục CNTT&Thống kê hải quan triển khai:

- Thực hiện đóng tất cả các cổng, dịch vụ, và các tính năng tương tự trên máy tính hay thiết bị mạng chưa sử dụng đối với các Hệ thống CNTT Hải quan tại DC, DR. Cổng TTĐT Hải quan.

- Hướng dẫn các đơn vị thuộc, trực thuộc TCHQ thực hiện đóng tất cả các cổng, dịch vụ, và các tính năng tương tự trên máy tính hay thiết bị mạng không dùng tới.

Các đơn vị thuộc, trực thuộc TCHQ triển khai:

- Triển khai thực hiện đóng tất cả các cổng, dịch vụ, và các tính năng tương tự trên máy tính, thiết bị mạng chưa sử dụng đối với các Hệ thống CNTT Hải quan tại TTDL&CNTT, phòng máy chủ; trang/cổng thông tin điện tử trong phạm vi quản lý của đơn vị.

đ) Quản lý kết nối

- Cục CNTT&Thống kê hải quan thực hiện quản lý kết nối mạng trong phạm vi toàn ngành; hỗ trợ tới Cục Hải quan các tỉnh, thành phố quản lý kết nối mạng trong phạm vi Cục Hải quan quản lý.

- Các đơn vị thuộc, trực thuộc TCHQ phối hợp với Cục CNTT&Thống kê hải quan trong việc theo dõi, cấp, thu hồi các quyền truy cập mạng của người dùng.

e) Quản lý định tuyến

Cục CNTT&Thống kê hải quan và Cục Hải quan các tỉnh, thành phố:

- Triển khai quản lý định tuyến mạng để bảo đảm các kết nối mạng máy tính và luồng thông tin không vi phạm chính sách quản lý truy cập.

- Triển khai quản lý định tuyến cần được dựa trên cơ chế kiểm tra địa chỉ nguồn và địa chỉ đích.

- Các cổng bảo vệ cần được kiểm tra để xác định địa chỉ nguồn và đích tại các thời điểm quản lý bên trong, bên ngoài mạng nếu các kỹ thuật chuyển đổi địa chỉ mạng và/hoặc máy trung gian được sử dụng. Cần hiểu biết tính đầy đủ và sự thiếu sót của cơ cấu được triển khai.

2. Quản lý truy cập Hệ điều hành

a) Các đơn vị thuộc, trực thuộc TCHQ

- Quản lý người dùng đã được cấp quyền truy cập hệ điều hành, phù hợp với chính sách quản lý truy cập đã xác định.

- Sau ba lần truy cập không thành công sẽ bị hủy quyền truy cập.

- Sau 5 phút truy cập không thành công sẽ bị hủy quyền truy cập.

- Ghi nhật ký việc sử dụng các đặc quyền của hệ thống.

- Ghi nhật ký những nỗ lực xác thực hệ thống thành công và thất bại.

b)Thủ tục đăng nhập an toàn

- Quản trị viên hệ thống:

+ Thực hiện đăng nhập, đăng xuất theo đúng tài khoản đã đăng ký;

+ Số lần đăng nhập tối đa ba (3) lần, quá ba lần đăng nhập, sẽ bị kết thúc đăng nhập.

- Người dùng:

+ Thực hiện đăng nhập, đăng xuất theo đúng tài khoản đã đăng ký; trong cùng thời điểm không được đăng nhập cùng một tài khoản trên nhiều máy tính khác nhau;

+ Số lần đăng nhập tối đa năm (5) lần, quá năm lần đăng nhập, sẽ bị kết thúc đăng nhập;

+ Không được đăng nhập từ tài khoản của người khác.

c) Định danh và xác thực người dùng

Tất cả những người dùng đều phải định danh duy nhất (định danh người dùng – User ID) để sử dụng riêng cho họ:

- Các ID của người dùng cần sử dụng để theo dõi các hoạt động của cá nhân. Không được thực hiện những hoạt động của người dùng thông qua các tài khoản đặc quyền, quản trị viên hệ thống.

- Trong trường hợp ngoại lệ, khi yêu cầu xử lý nghiệp vụ, có thể sử dụng ID người dùng chia sẻ một nhóm người dùng hoặc một công việc nhất định, được lãnh đạo đơn vị phê duyệt.

- Khi có yêu cầu xác thực mạnh hoặc xác minh định danh thì thực hiện các phương thức xác thực thay thế mật khẩu, ví dụ các phương tiện mã hóa, thẻ thông minh, thẻ hoặc các phương tiện sinh trắc học hay mã thông báo sẽ được sử dụng.

d) Hệ thống quản lý mật khẩu

- Bắt buộc sử dụng các ID và mật khẩu cá nhân riêng để duy trì khả năng giải trình trách nhiệm.

- Triển khai các quy định về quản lý mật khẩu.

đ) Giới hạn thời gian phiên làm việc

- Các phiên làm việc không hoạt động sẽ đóng lại sau thời gian không hoạt động là 15 phút.

- Khi tạm ngừng làm việc, phải đăng xuất hoặc khóa màn hình.

Điều 17. Vận hành và giám sát hệ thống mạng

1. Trách nhiệm Cục CNTT&Thống kê hải quan

- Xây dựng, trình cấp có thẩm quyền ban hành quy trình vận hành, giám sát hoạt động của Hệ thống mạng Hải quan;

- Thực hiện giám sát hoạt động của Hệ thống mạng diện rộng (WAN), trên phạm vi toàn ngành Hải quan;

- Thực hiện trực, giám sát hoạt động của hệ thống mạng hải quan 24/24 h các ngày, đồng thời nghiên cứu triển khai thiết bị giám sát hoạt động hệ thống mạng (kết hợp với tiếp nhận thông báo qua điện thoại, mail), đưa ra thông báo kịp thời về tình trạng của mạng; khi bị gián đoạn hoạt động mạng đưa ra địa chỉ, thời gian bị gián đoạn, để tổ chức chỉ đạo khắc phục ngay sự cố;

- Hướng dẫn các đơn vị thuộc, trực thuộc TCHQ vận hành, giám sát, khắc phục sự cố với hệ thống mạng trong phạm vi đơn vị chủ trì quản lý.

2. Trách nhiệm của Cục Hải quan các tỉnh, thành phố

- Thực hiện vận hành, trực giám sát hoạt động của Hệ thống mạng WAN, LAN trên địa bàn (phạm vi) đơn vị được giao chủ trì quản lý theo đúng quy trình vận hành, giám sát hệ thống mạng.

- Thông báo ngay các sự cố về mạng máy tính về TCHQ (Cục CNTT&Thống kê hải quan) để triển khai các biện pháp khắc phục.

- Khi có sự cố xảy ra, đơn vị phải triển khai ngay biện pháp khắc phục, bảo đảm hệ thống mạng hoạt động liên tục, phục vụ công tác.

- Phối hợp với Cục CNTT&Thống kê hải quan trong vận hành, giám sát, khắc phục sự cố về mạng máy tính, triển khai các biện pháp kỹ thuật trong vận hành, giám sát hoạt động của mạng máy tính.

3. Trách nhiệm của các đơn vị thuộc Tổng cục Hải quan

- Thực hiện giám sát hoạt động của Hệ thống mạng LAN triển khai tại đơn vị;

- Thông báo ngay các sự cố về mạng máy tính về TCHQ (Cục CNTT&Thống kê hải quan) để triển khai các biện pháp khắc phục.

MỤC 3
PHẦN MỀM ỨNG DỤNG

Điều 18. Quy định bảo đảm an ninh, an toàn khi vận hành, giám sát hoạt động của phần mềm ứng dụng

1. Quy định bảo đảm an ninh, an toàn khi vận hành phần mềm ứng dụng

a) Trách nhiệm của Cục CNTT&Thống kê hải quan

- Xây dựng, trình cấp có thẩm quyền ban hành quy trình vận hành, giám sát đối với từng phần mềm ứng dụng;

- Vận hành các phần mềm ứng dụng triển khai tại DC, DR và Cổng TTĐT Hải quan;

- Bảo đảm các ứng dụng hoạt động liên tục 24/24h tất cả các ngày;

- Hỗ trợ các đơn vị hải quan thuộc, trực thuộc TCHQ vận hành, xử lý các sự cố liên quan đến vận hành, giám sát phần mềm ứng dụng.

b) Trách nhiệm của Cục Hải quan các tỉnh, thành phố

- Vận hành các phần mềm ứng dụng do đơn vị quản lý, triển khai tại TTDL&CNTT, phòng máy chủ thuộc Cục, Chi cục; vận hành hoạt động trang/cổng thông tin điện tử của đơn vị;

- Bảo đảm các ứng dụng hoạt động liên tục 24/24h tất cả các ngày;

- Thực hiện đúng thao tác vận hành ứng dụng đã quy định trong các quy trình vận hành quy định cho từng phần mềm ứng dụng;

- Hỗ trợ các chi cục Hải quan trực thuộc vận hành các phần mềm ứng dụng, triển khai tại Chi cục hải quan;

- Thực hiện báo cáo, kiến nghị vướng mắc quá trình bảo đảm an ninh, an toàn khi vận hành phần mềm ứng dụng về TCHQ (Cục CNTT&Thống kê hải quan) để kịp thời khắc phục vướng mắc và triển khai quy định mới cho phù hợp.

c) Trách nhiệm của các đơn vị thuộc TCHQ

- Vận hành các phần mềm ứng dụng, trang/cổng thông tin điện tử do đơn quản lý;

- Bảo đảm các ứng dụng hoạt động liên tục 24/24h tất cả các ngày;

- Thực hiện đúng thao tác vận hành phần mềm ứng dụng;

- Thực hiện báo cáo, kiến nghị vướng mắc quá trình bảo đảm an ninh, an toàn vận phần mềm ứng dụng về TCHQ (Cục CNTT&Thống kê hải quan) để kịp thời khắc phục vướng mắc và triển khai quy định mới cho phù hợp.

2. Bảo đảm an ninh, an toàn trong giám sát hoạt động của phần mềm ứng dụng

a) Trách nhiệm của Cục CNTT&Thống kê hải quan

- Tổ chức trực giám sát hoạt động của các phần mềm ứng dụng đã triển khai tại DC, DR; Cổng TTĐT Hải quan;

- Triển khai công nghệ trong hoạt động giám sát tập trung các hoạt động, kịp thời phát hiện các sự cố về hoạt động của phần mềm ứng dụng, có biện pháp khắc phục để bảo đảm các hoạt động liên tục;

- Hướng dẫn, hỗ trợ các đơn vị hải quan thuộc, trực thuộc TCHQ thực hiện giám sát hoạt động của các phần mềm ứng dụng, trang/cổng thông tin điện tử của các đơn vị;

b) Trách nhiệm của Cục Hải quan các tỉnh, thành phố

- Tổ chức trực giám sát hoạt động của các phần mềm ứng dụng đã triển khai tại TTDL&CNTT, phòng máy chủ, trang/cổng thông tin điện tử của đơn vị;

- Phối hợp với Cục CNTT&Thống kê hải quan triển khai công nghệ trong hoạt động giám sát tập trung hoạt động của các phần mềm ứng dụng, kịp thời phát hiện các sự cố về hoạt động của ứng dụng, báo cáo về TCHQ (Cục CNTT&Thống kê hải quan) để triển khai các biện pháp khắc phục.

- Hướng dẫn, hỗ trợ các đơn vị hải quan thuộc, trực thuộc Cục thực hiện giám sát hoạt động của các phần mềm ứng dụng, báo cáo về Cục các sự cố liên quan đến hoạt động của phần mềm ứng dụng.

c) Trách nhiệm của các đơn vị thuộc TCHQ

- Tổ chức trực giám sát hoạt động của các phần mềm ứng dụng, trang/cổng thông tin điện tử của đơn vị;

- Phối hợp với Cục CNTT&Thống kê hải quan triển khai công nghệ trong hoạt động giám sát tập trung hoạt động của các phần mềm ứng dụng, kịp thời phát hiện các sự cố về hoạt động của phần mềm ứng dụng, báo cáo về TCHQ (Cục CNTT&Thống kê hải quan) để triển khai các biện pháp khắc phục.

Điều 19. Quy định an ninh, an toàn đối với việc khai thác, sử dụng thông tin từ dữ liệu điện tử hải quan

1. Cục CNTT&Thống kê hải quan

- Xây dựng, trình cấp thẩm quyền ban hành quy trình khai thác số liệu nghiệp vụ trên các phần mềm ứng dụng;

- Chủ trì khai thác dữ liệu đầu ra của các phần mềm ứng dụng, phục vụ công tác nghiệp vụ và Thống kê Nhà nước về Hải quan;

- Hướng dẫn các đơn vị thuộc, trực thuộc TCHQ khai thác dữ liệu đầu ra của các phần mềm ứng dụng, phục vụ công tác nghiệp vụ;

- Kiểm soát các truy cập để khai thác dữ liệu đầu ra của các phần mềm ứng dụng, kịp thời thông báo tới các đơn vị những vấn đề cần thiết để tăng cường biện pháp quản lý số liệu.

2. Các đơn vị thuộc, trực thuộc TCHQ

- Thực hiện khai thác dữ liệu trên các phần mềm ứng dụng để phục vụ công tác nghiệp vụ, quản lý của đơn vị;

- Chịu trách nhiệm kiểm tra, giám sát cán bộ, công chức, viên chức thuộc đơn vị tham gia khai thác, sử dụng dữ liệu đúng mục đích công việc;

- Chịu trách nhiệm quản lý, bảo mật số liệu đã thực hiện khai thác trên các phần mềm ứng dụng theo các quy định hiện hành;

- Thông báo về TCHQ (Cục CNTT&Thống kê hải quan) những yêu cầu phát sinh, kiến nghị, cả những vấn đề cần phối hợp quản lý để bảo đảm an toàn an ninh cho dữ liệu đã tham gia khai thác.

Điều 20. Quy định an ninh, an toàn sao lưu dữ liệu điện tử hải quan

Cục CNTT&Thống kê hải quan chủ trì sao lưu Hệ thống CNTT hải quan triển khai tại các DC, DR, Cổng TTĐT Hải quan và hỗ trợ, hướng dẫn cho các Cục Hải quan tỉnh, thành phố thực hiện sao lưu, phục hồi dữ liệu.

Các đơn vị thuộc, trực thuộc TCHQ chủ trì sao lưu, phục hồi dữ liệu các Hệ thống CNTT hải quan triển khai tại đơn vị (TTDL&CNTT, Phòng máy chủ tại đơn vị, Chi cục hải quan); trang/cổng thông tin điện tử do đơn vị quản lý.

Nội dung sao lưu phục hồi dữ liệu như sau:

1. Quy định việc Tổ chức sao- phục hồi sao lưu

Lãnh đạo đơn vị chủ trì quản lý Hệ thống CNTT Hải quan phê duyệt:

a) Kế hoạch sao lưu, phục hồi dữ liệu *(kế hoạch quy định rõ thời gian, địa điểm, nội dung sao toàn bộ hay từng phần chương trình và dữ liệu, phương pháp sao lưu, phục hồi dữ liệu).*

b) Kế hoạch đảm bảo an toàn - an ninh trong sao lưu, phục hồi dữ liệu;

c) Nội dung thực hiện kiểm thử các biện pháp sao lưu, phục hồi dữ liệu trước khi áp dụng vào hệ thống thật.

d) Xây dựng, phổ biến tài liệu hướng dẫn, biện pháp an toàn khi sao lưu, phục hồi dữ liệu.

2. Bảo đảm an ninh, an toàn vận hành sao lưu

a) Thực hiện các biện pháp sau đây để đảm bảo việc vận hành sao lưu, phục hồi dữ liệu được thông suốt

- Thiết lập hệ thống mạng dự phòng cho sao lưu;

- Chuẩn bị thiết bị thay thế dự phòng cho hệ thống sao lưu dữ liệu;

- Sử dụng các thiết bị và chuẩn kết nối tốc độ cao;

- Đảm bảo khả năng lưu trữ các bản sao dữ liệu;

- Xây dựng hệ thống kiểm thử cho việc sao lưu, phục hồi dữ liệu.

b) Thực hiện đảm bảo việc sao lưu dữ liệu được thực hiện chính xác

- Kiểm tra trạng thái hệ thống trước và sau khi sao lưu dữ liệu;

- Kiểm tra, xác định chính xác dữ liệu cần sao lưu và nơi lưu trữ bản sao dữ liệu;

- Kiểm tra dữ liệu trước và sau khi sao lưu;

- Thực hiện kiểm thử trước khi tiến hành sao lưu.

c) Phải thực hiện các công việc sau đây để đảm bảo việc phục hồi dữ liệu được thực hiện chính xác

- Kiểm tra trạng thái hệ thống trước và sau khi phục hồi dữ liệu;

- Kiểm tra, xác định chính xác dữ liệu cần phục hồi trước khi thực hiện phục hồi dữ liệu;

- Kiểm tra dữ liệu trước và sau khi phục hồi;

- Thực hiện kiểm thử trước khi phục hồi dữ liệu.

3. Bảo đảm an ninh, an toàn trong thực hiện sao lưu

a) Thực hiện đúng biện pháp, quy trình khi sao lưu, phục hồi dữ liệu.

b) Thực hiện đánh giá 6 tháng/lần mức độ an toàn trong sao lưu, phục hồi dữ liệu; đề xuất các thay đổi nhằm nâng cao mức an toàn.

4. Bảo đảm an ninh, an toàn cho bản sao lưu

a) Các biện pháp đảm bảo an toàn cho bản sao dữ liệu:

- Cấu hình RAID trên các máy chủ và trên hệ thống lưu trữ mở rộng sử dụng đĩa cứng;

- Chuẩn bị thiết bị lưu trữ dự phòng để thay thế cho các thiết bị không còn khả năng sử dụng;

- Sử dụng tủ lưu trữ chống cháy và có khóa để lưu trữ dữ liệu.

- Kiểm soát, phân quyền các truy nhập vật lý và truy nhập từ xa tới bản sao dữ liệu.

b) Hủy bỏ các thiết bị lưu trữ bản sao dữ liệu không còn khả năng sử dụng.

Điều 21. Quy định an ninh, an toàn khi sử dụng mật khẩu

1. Quy định trách nhiệm quản lý mật khẩu

a) Quy định chung, phân loại và nguyên tắc cấp mật khẩu

- Quy định chung về mật khẩu: các phần mềm quản trị hệ thống; phần mềm ứng dụng; phần mềm quản trị cơ sở dữ liệu; hệ thống an ninh an toàn đều có hệ thống mật khẩu riêng (một mật khẩu đặc quyền, các mật khẩu quản trị và mật khẩu người dùng, nhóm người dùng).

- Trách nhiệm quản lý mật khẩu:

+ Cục CNTT&Thống kê hải quan quản lý, cấp phát, thu hồi mật khẩu đặc quyền, mật khẩu quản trị hệ thống, mật khẩu người dùng, nhóm người dùng với các Hệ thống CNTT triển khai tại DC và DR; Cổng TTĐT Hải quan.

+ Cục Hải quan các tỉnh, thành phố quản lý, cấp phát, thu hồi mật khẩu đặc quyền, mật khẩu quản trị hệ thống, mật khẩu người dùng, nhóm người dùng với các Hệ thống CNTT triển khai tại TTDL&CNTT, Phòng máy chủ các đơn vị

thuộc Cục; trang/cổng thông tin điện tử do đơn vị quản lý. Quản lý mật khẩu quản trị, mật khẩu người dùng đã đăng ký và được cấp tài khoản truy cập.

+ Các đơn vị thuộc cơ quan TCHQ: Quản lý, cấp phát, thu hồi mật khẩu đặc quyền, mật khẩu quản trị hệ thống, mật khẩu người dùng, nhóm người dùng với các Hệ thống CNTT, trang/cổng thông tin điện tử do đơn vị chủ trì quản lý. Quản lý mật khẩu quản trị, mật khẩu người dùng đã đăng ký và được được cấp tài khoản truy cập vào các Hệ thống CNTT Hải quan.

b) Nguyên tắc quản lý, cấp mật khẩu

- Mật khẩu đặc quyền: Tại TCHQ do Cục trưởng Cục CNTT và Thống kê quản lý hoặc phân công quản lý; tại các đơn vị thuộc, trực thuộc TCHQ do Trưởng TTDL&CNTT hoặc trưởng đơn vị phụ trách Bộ phận CNTT quản lý;

- Mật khẩu quản trị: Cấp cho quản trị viên của từng hệ thống (quản trị viên hệ thống, quản trị viên ANTT, quản trị viên ứng dụng, quản trị viên quản trị cơ sở dữ liệu).

- Mật khẩu người dùng, nhóm người dùng: cấp cho người sử dụng trong các Hệ thống CNTT Hải quan.

- Nguyên tắc cấp: Một cán bộ, công chức, viên chức không làm quản trị đồng thời hai hệ thống, hai ứng dụng (*quản trị viên hệ thống, quản trị viên ANTT, quản trị viên ứng dụng, quản trị viên quản trị cơ sở dữ liệu*).

2. Quy định quản lý mật khẩu

a) Đăng ký người dùng

- Cán bộ, công chức, viên chức đăng ký và sử dụng các ID người dùng duy nhất; việc sử dụng ID nhóm chỉ được thực hiện khi có sự phê duyệt của lãnh đạo đơn vị;

- Đơn vị được giao quản lý hệ thống CNTT thực hiện:

+ Kiểm tra người dùng đã được cấp quyền truy cập sử dụng hệ thống hoặc dịch vụ thông tin;

+ Kiểm tra các quyền truy cập được cấp có phù hợp mục đích nghiệp vụ và phù hợp chính sách an ninh của cơ quan không;

+ Thiết lập hồ sơ quản lý tất cả các người đã đăng ký sử dụng dịch vụ;

+ Loại bỏ hoặc ngăn chặn kịp thời các quyền truy cập của những người dùng đã tạm ngừng, nghỉ hoặc thay đổi vị trí công việc;

+ Kiểm tra định kỳ, loại bỏ hoặc chặn các ID người dùng và các tài khoản thừa;

+ Đảm bảo rằng các ID thừa không được cấp cho những người khác.

b) Quy định chung khi sử dụng mật khẩu

- Giữ bí mật mật khẩu, không cho người khác biết;

- Tránh giữ hồ sơ (giấy, tập tin phần mềm hoặc thiết bị cầm tay) có ghi mật khẩu, trừ khi hồ sơ được giữ an toàn và phương pháp lưu giữ được phê duyệt;

- Mật khẩu đặt theo tiêu chí mật khẩu mạnh:

+ Có ít nhất 8 ký tự;

+ Chứa từ 3 trong 4 loại ký tự sau: chữ hoa (A, B, C...), chữ thường (a,b,c), chữ số (0, 1, 2...), ký tự đặc biệt (@#...); riêng đối với VNACCS/VCIS chưa sử dụng ký tự đặc biệt.

+ Không chứa tất cả hoặc một phần tên tài khoản người dùng tương ứng;

+ Không sử dụng: ngày sinh nhật, tên đầu hoặc cuối, tên viết tắt, tên vợ con, tên cơ quan, số điện thoại, v.v... .

+ Không dễ tổn hại bởi những tấn công dò tìm mật khẩu thông qua từ điển (tức là không chứa các từ trong từ điển);

+ Không phải là dãy ký tự hay số giống nhau liên tiếp.

- Thực hiện thay đổi mật khẩu định kỳ: 6 tháng /lần đối với tài khoản của người dùng; 3 tháng /lần đối với tài khoản quản trị hệ thống;

- Không sử dụng chung mật khẩu của ứng dụng nghiệp vụ với các ứng dụng cá nhân;

- Khi kết thúc công việc phải thực hiện việc đăng xuất;

- Khi bị lộ mật khẩu, hoặc nghi ngờ bị lộ mật khẩu phải đổi mật khẩu và báo cáo ngay cán bộ quản trị để thực hiện khóa ngay tài khoản, nhằm ngăn chặn các hành động phá hoại, lấy cắp thông tin, lợi dụng tín nhiệm;

- Nếu quên mật khẩu, người sử dụng thực hiện theo quy trình cấp mật khẩu mới;

- Khi sử dụng mật khẩu mới, phải đổi sang mật khẩu khác;

- Không đưa mật khẩu vào thủ tục đăng nhập tự động, ví dụ đăng ký trong chương trình macro hay khóa chức năng;

- Không chia sẻ mật khẩu người dùng cá nhân.

c) Quy định quản lý mật khẩu đặc quyền

- Tuân thủ Quy định chung khi sử dụng mật khẩu;

- Mật khẩu đặc quyền được quản lý, bảo mật, lưu trữ bằng các biện pháp đặc biệt: lưu ra giấy (có đặt khóa mã hóa riêng); mật khẩu và mã khóa riêng của mật khẩu được niêm phong độc lập trong phong bì và cất độc lập trong các tủ hoặc két có mã khóa;

- Người quản lý mật khẩu đặc quyền được phép tạo ra tài khoản có đặc quyền cao để dự phòng; Mật khẩu của tài khoản này phải được lưu giữ với độ an toàn bảo mật cao như mật khẩu đặc quyền. Mật khẩu này được cất trữ riêng biệt, không lưu trong các hệ thống quản lý tự động; không cất cùng với mật khẩu đặc quyền;

- Mật khẩu đặc quyền các máy chủ của trang/cổng thông tin điện tử hải quan (thuê chỗ ngoài): do lãnh đạo đơn vị cấp Phòng, TTDL trực tiếp quản lý và tuân thủ theo nguyên tắc quản lý mật khẩu đặc quyền tại mục (a,b) khoản này;

- Người quản lý mật khẩu đặc quyền được phép tạo ra một mật khẩu có đặc quyền cao, đủ để thực hiện nhiệm vụ cấp mới, thu hồi mật khẩu quản trị, mật khẩu người sử dụng theo thẩm quyền được quy định;

- Mật khẩu đặc quyền và mật khẩu có đặc quyền cao để dự phòng không sử dụng trong thực tế, chỉ được sử dụng trong các trường hợp đặc biệt: Khắc phục sự cố khẩn cấp hoặc sử dụng trong các trường hợp khác đã được Lãnh đạo đơn vị phê duyệt, chỉ đạo.

d) Quy định quản lý mật khẩu quản trị

- Tuân thủ Quy định chung khi sử dụng mật khẩu.

- Lưu trữ mật khẩu bằng các biện pháp an toàn, mã hóa mật khẩu trong quá trình lưu trữ và truyền tải qua mạng.

- Mật khẩu mặc định của nhà sản xuất (mới cấp) phải được thay đổi ngay lập tức sau khi đưa vào hoạt động.

- Mật khẩu quản trị trong Hệ thống CNTT Hải quan, chỉ thực hiện truy cập vào Hệ thống từ các máy tính dùng cho quản trị viên Hệ thống trong khu vực phục kiểm soát an ninh thông tin, có xác thực mạnh.

- Mật khẩu quản trị khi truy cập từ xa (bên ngoài) vào Hệ thống CNTT Hải quan chỉ được thực hiện khi lãnh đạo đơn vị phân công, chỉ đạo cho thực hiện, khi truy cập từ xa phải thực hiện các biện pháp xác thực đa nhân tố, và thực hiện trên các phương tiện xử lý thông tin đã có các Hệ thống bảo đảm an ninh, an toàn.

- Phải thực hiện đăng xuất trong vòng 30 phút đối với tài khoản người dùng và 15 phút đối với tài khoản quản trị khi không sử dụng.

- Ghi nhật ký (log) đăng nhập và thay đổi mật khẩu.

đ) Quy định quản lý mật khẩu người dùng

-Tuân thủ Quy định chung khi sử dụng mật khẩu.

- Người dùng phải có tài khoản cá nhân, bao gồm tên đăng nhập và mật khẩu, để xác thực và quản lý định danh người dùng khi tham gia vào hệ thống CNTT Hải quan.

- Người dùng có một mật khẩu tạm thời an toàn và phải được thay đổi ngay lập tức sau lần sử dụng đầu tiên. Mật khẩu tạm thời phải là duy nhất, không được tái sử dụng và phải tuân thủ với yêu cầu về cách thức chọn.

- Thực hiện biện pháp an toàn để cung cấp mật khẩu tạm thời cho người dùng, ví dụ: phong bì đảm bảo dán kín có niêm phong, qua các kênh trao đổi thông tin nội bộ có mã hóa, v.v.. .

- Việc cấp phát lại mật khẩu cần đảm bảo đúng quy trình cấp mật khẩu mới.

- Trong một số trường hợp người dùng đòi hỏi yêu cầu bảo mật cao, cần triển khai biện pháp xác thực đa nhân tố, tối thiểu là hai nhân tố.

3. Kiểm tra quyền truy cập mật khẩu

a) Kiểm tra định kỳ 3 tháng một lần các quyền truy cập của quản trị viên, 6 tháng một lần các quyền truy cập người dùng, và khi có thay đổi bất kỳ, ví dụ được đề bạt, bị giáng chức hoặc kết thúc công việc, thì phải sửa hoặc thu hồi quyền truy cập.

b) Kiểm tra các mật khẩu có đặc quyền truy cập, tải khoản nhóm để bảo đảm truy cập đúng mục đích công việc.

e) Ghi nhật ký kiểm tra quyền truy cập (ghi biên bản).

Điều 22. Đảm bảo an ninh, an toàn truy cập Internet

1. Trách nhiệm Cục CNTT&Thống kê hải quan, Cục Hải quan các tỉnh, thành phố

a) Duy trì kết nối Internet tại cơ quan Tổng cục Hải quan; văn phòng Cục Hải quan các tỉnh, thành phố, bảo đảm đủ băng thông khi truy cập; khắc phục khi bị sự cố trên mạng internet.

b) Thiết lập các giải pháp bảo đảm an ninh, an toàn đối với mạng nội bộ khỏi các nguy cơ từ môi trường Internet: quy định khu vực máy tính được kết nối internet; xây dựng tường lửa bảo vệ đường vào, ra internet.

c) Thiết lập giải pháp lọc nội dung, giải pháp nhằm đảm bảo ngăn chặn việc lạm dụng kết nối Internet vào các mục đích cá nhân; tối ưu băng thông dữ liệu tải lên và tải về.

d) Tuân thủ theo quy định kiểm tra và báo cáo.

2. Trách nhiệm các đơn vị thuộc, trực thuộc TCHQ

a) Phê duyệt danh sách cán bộ được phép truy nhập Internet.

b) Quản lý, hướng dẫn việc sử dụng Internet của công chức, viên chức thuộc đơn vị đúng với mục đích nghiệp vụ.

c) Thực hiện đúng trách nhiệm cụ thể khi sử dụng internet.

3. Trách nhiệm khai thác thông tin trên internet

Cán bộ, công chức, viên chức:

a) Nghiêm cấm sử dụng máy tính trong các dây chuyền nghiệp vụ truy cập vào internet.

b) Chỉ thực hiện truy cập vào internet từ các máy tính đã được cấp quyền truy cập; sử dụng các thông tin trên internet vào các mục đích công việc của cơ quan.

c) Nghiêm cấm máy tính dùng để soạn thảo, in ấn, lưu trữ bí mật Nhà nước, các tệp dữ liệu chuẩn (CSF tiêu chí quản lý rủi ro, danh mục rủi ro về giá v.v...) của các chương trình nghiệp vụ kết nối vào Internet.

Điều 23. Đảm bảo an ninh, an toàn hệ thống thư điện tử

1. Quy định sử dụng thư điện tử

Cán bộ, công chức, viên chức:

a) Sử dụng hộp thư điện tử của Ngành có tên miền (.customs.gov.vn) để trao đổi, phục vụ công việc của cơ quan.

b) Không sử dụng thư điện tử của Ngành để thực hiện các mục đích, các hoạt động không hợp pháp; tham gia diễn đàn công cộng.

c) Khi trao đổi thông tin qua thư điện tử, nếu nhận được file đính kèm từ một hộp thư không biết, hoặc file đính kèm có định dạng: .exe, .com, .scr, .pif, .bat, .cmd, .vbs thì phải sử dụng các phần mềm quét, phát hiện ngăn chặn mã độc trước khi mở chúng, hoặc thông báo cho người quản trị biết.

d) Tất cả các máy cá nhân sử dụng để trao đổi thông tin bằng thư điện tử phải được cài đặt các phần mềm phòng chống mã độc, virus ... .

e) Không được phép cố ý gửi và lưu chuyển thư điện tử đã nhiễm mã độc hại. Cấm chuyển tiếp các loại thư điện tử rác có nội dung độc hại và các loại thư điện tử chứa mã tự động chạy hoặc có khả năng tự thực thi (file flash, exe...).

f) Công chức, viên chức không được phép truy nhập tài khoản thư điện tử cá nhân của người khác (chỉ trừ khi được phép của cấp có thẩm quyền).

g) Thường xuyên xem lại các thư điện tử được lưu trữ và xoá các thư điện tử với nội dung không cần thiết để tiết kiệm dung lượng lưu trữ.

h) Sau khi được bàn giao tài khoản thư điện tử, người dùng phải thay đổi ngay lập tức mật khẩu mặc định cho tài khoản đó.

i) Phải thực hiện đăng xuất (log-out) sau khi kết thúc công việc trên hệ thống thư điện tử.

2. Quy định quản trị thư điện tử

Cục CNTT&Thống kê hải quan quản lý Hệ thống thư điện tử:

a) Thực hiện cơ chế cảnh báo về an toàn thông tin cho người dùng thư điện tử (ví dụ: dung lượng không đủ để gửi nhận, thư điện tử không gửi tới nơi,...);

b) Cấp dung lượng lưu trữ trong thư điện tử phù hợp với chức vụ, yêu cầu nghiệp vụ của cán bộ, viên chức;

c) Triển khai các cơ chế xác thực đối với các tài khoản người dùng trong việc nhận và gửi các thông tin qua thư điện tử, chẳng hạn như việc sử dụng mật khẩu "mạnh", sử dụng chữ ký số, ... ;

d) Thực hiện biên pháp lọc chặn: lọc chặn thư rác, lọc chặn các nội dung không phù hợp v.v... ;

e) Thực hiện các chính sách về quản lý mật khẩu người dùng theo quy định;

f) Thực hiện các biện pháp bảo mật cho máy chủ thư điện tử;

g) Báo cáo lãnh đạo đơn vị về các trường hợp xâm phạm, xem trộm thư cá nhân người khác;

h) Cấm không được chia sẻ mật khẩu quản trị của hệ thống thư điện tử.

Điều 24. Quy định bảo vệ chống lại mã độc và mã di động

1. Quy định triển khai các phần mềm chống mã độc hại, di động

a) Triển khai giải pháp phòng chống mã độc

Cục CNTT&Thống kê hải quan:

- Triển khai các giải pháp phòng chống mã độc hại; cài đặt chương trình tìm, phát hiện, diệt mã độc trên máy tính thuộc DC và DR thuộc TCHQ; hỗ trợ Cục Hải quan các tỉnh, thành phố triển khai chương trình phòng chống mã độc trên các may tính của đơn vị;

- Sử dụng hai hoặc nhiều sản phẩm phần mềm phòng chống mã độc của các nhà cung cấp khác nhau để nâng cao hiệu quả phòng chống mã độc;

- Tiếp nhận thông báo về sự cố liên quan đến mã độc hại từ các đơn vị thuộc, trực thuộc Tổng cục Hải quan;

- Xác định nguyên nhân và đề ra biện pháp xử lý mã độc.

- Thực hiện các biện pháp xử lý sự cố liên quan đến mã độc hại trên máy trạm và máy chủ;

- Khôi phục hoạt động hệ thống sau khi xử lý sự cố liên quan đến mã độc hại.

Cục Hải quan các tỉnh thành phố:

- Triển khai các giải pháp phòng chống mã độc hại; cài đặt chương trình tìm, phát hiện, diệt mã độc hại trên các máy tính thuộc Cục Hải quan quản lý;

- Tiếp nhận thông báo về sự cố liên quan đến mã độc hại từ các Phòng, Ban, Chi cục hải quan trực thuộc, báo cáo về TCHQ;

- Phối hợp với Cục CNTT&Thống kê hải quan, triển khai các biện pháp xử lý sự cố liên quan đến mã độc hại trên máy trạm và máy chủ;

- Khôi phục hoạt động các máy tính thuộc Cục (Phòng, Ban, Chi cục) sau khi xử lý sự cố liên quan đến mã độc hại.

b) Trách nhiệm của các đơn vị quản lý trong việc bảo vệ chống lại mã độc của các đơn vị:

- Quản lý, theo dõi các giải pháp phòng chống mã độc hại và đảm bảo các giải pháp này vận hành liên tục;

- Theo dõi và phát hiện sớm nguồn phát tán mã độc hại để kịp thời xử lý;

- Báo cáo Tổng cục Hải quan khi các giải pháp phòng chống mã độc hại không hoạt động hoặc hoạt động không đúng chức năng và khi xảy ra sự cố liên quan đến mã độc hại;

- Tổ chức các đơn vị có liên quan trong việc xử lý các sự cố liên quan đến mã độc hại.

2. Quy định bảo vệ chống lại mã độc và mã di động

Cán bộ, công chức, viên chức thực hiện:

a) Không được sử dụng phần mềm trái phép.

b) Nâng cao công tác bảo vệ bí mật Nhà nước, không được sử dụng các thiết bị di động thông minh (điện thoại thông minh Smartphone, máy tính bảng, thiết bị thu phát media...) vừa kết nối vào internet vừa kết nối vào mạng của cơ quan hải quan, hoặc lưu trữ các bí mật nhà nước.

c) Không mang các thiết bị di động thông minh vào các cuộc họp có nội dung bí mật, hạn chế đến mức thấp nhất việc sử dụng các thiết bị di động thông minh và dịch vụ trực tuyến tại nơi làm việc.

d) Để chế độ tự động kiểm tra, quét phát hiện mã độc trên các chương trình quét mã độc hại để quét máy tính và các phương tiện xử lý thông tin để phát hiện, ngăn chặn mã độc. Hàng tuần kiểm tra sự hoạt động của chương trình quét mã độc hại.

Điều 25. Đánh giá an ninh, an toàn Hệ thống CNTT Hải quan

1. Quy định trách nhiệm

a) Trách nhiệm của Cục CNTT&Thống kê hải quan

- Triển khai nội dung kiểm tra lỗ hổng bảo mật đối với các Hệ thống CNTT Hải quan một năm/lần; phần mềm ứng dụng quan trọng 6 tháng/lần.

- Thực hiện khắc phục lỗ hổng bảo mật với các Hệ thống CNTT triển khai tại các DR, DC; Cổng TTĐT Hải quan;

- Thông báo, hướng dẫn nội dung cần khắc phục tới các đơn vị thuộc, trực thuộc TCHQ thực hiện khắc phục lỗ hổng bảo mật đối với Hệ thống CNTT Hải quan triển khai, do đơn vị hải quan chủ trì quản lý.

- Tổng hợp kết quả, báo cáo của các đơn vị thuộc, trực thuộc TCHQ; báo cáo Lãnh đạo TCHQ, Lãnh đạo Bộ Tài chính theo định kỳ tháng 6 và tháng 12 hàng năm, và các báo cáo đột xuất.

b) Trách nhiệm của Cục Hải quan các tỉnh, thành phố

- Khi có thông báo từ Cục CNTT&Thống kê hải quan, thực hiện khắc phục lỗ hổng bảo mật với các Hệ thống CNTT Hải quan triển khai tại Cục Hải quan, Chi cục hải quan trực thuộc; trang/cổng TTĐT Hải quan do đơn vị quản lý;

- Báo cáo kết quả khắc phục lỗ hổng bảo mật về TCHQ (Cục CNTT&Thống kê hải quan) tổng hợp báo cáo TCHQ, Bộ Tài chính trước ngày 20/6 và 20/12 hàng năm; các báo cáo kiểm tra chấp hành hệ thống; báo cáo đột xuất.

c) Trách nhiệm các đơn vị thuộc cơ quan TCHQ

- Khi có thông báo từ Cục CNTT&Thống kê hải quan, thực hiện khắc phục lỗ hổng bảo mật với các Hệ thống CNTT Hải quan; trang/cổng thông tin điện tử do đơn vị triển khai, quản lý.

- Báo cáo kết quả khắc phục lỗ hổng bảo mật về TCHQ (Cục CNTT&Thống kê hải quan) tổng hợp báo cáo TCHQ, Bộ Tài chính trước ngày 20/6 và 20/12 hàng năm; các báo cáo kiểm tra chấp hành hệ thống; báo cáo đột xuất.

2. Đánh giá hệ thống, an ninh an toàn hệ thống thông tin

a) Cục CNTT&Thống kê hải quan căn cứ kết quả kiểm tra, khắc phục lỗ hổng bảo mật của Cục và các đơn vị thuộc, trực thuộc TCHQ, tổng hợp xây dựng báo cáo đánh giá an ninh, an toàn Hệ thống CNTT Hải quan theo định kỳ sáu tháng, một năm.

b) Đề xuất các giải pháp kỹ thuật tiên tiến, triển khai các biện pháp để kiểm soát, bảo đảm an ninh, an toàn các Hệ thống CNTT Hải quan.

Điều 26. Quy định hoạt động liên tục của hệ thống

1. Cục CNTT&Thống kê hải quan, thực hiện

a) Xây dựng Kế hoạch, quy trình, quy chế bảo đảm hoạt đông liên tục đối với các hệ thống CNTT quan trọng của ngành Hải quan;

b) Danh sách các hệ thống quan trọng của Ngành được xác định:

- Phần mềm xử lý dữ liệu tập trung;

- Một số phần mềm xử lý dữ liệu phân tán triển khai toàn Ngành (do Cục CNTT&Thống kê hải quan) xác định từng năm;

- Các trang/cổng thông tin điện tử trong ngành Hải quan.

c) Kiểm tra giám sát và báo cáo

- Kiểm tra, giám sát, đánh giá việc thực hiện công tác thực hiện đảm bảo hoạt động liên tục của hệ thống CNTT 6 tháng/lần;

- Báo cáo lên Lãnh đạo TCHQ việc thực hiện Kế hoạch công tác bảo đảm hoạt động liên tục của Hệ thống CNTT Hải quan, định kỳ 6 tháng/lần.

2. Nội dung bảo đảm hoạt động liên tục

a) Lãnh đạo đơn vị phê duyệt Kế hoạch, quy trình đảm bảo hoạt động liên tục đối với hệ thống CNTT do đơn vị chủ trì quản lý.

b) Một Lãnh đạo đơn vị thường trực trong công tác đảm bảo hoạt động liên tục đối với Hệ thống CNTT Hải quan.

c) Công tác thực hiện đảm bảo tính liên tục hệ thống CNTT phải được thực hiện bởi các thành viên đã được phân công.

d) Có đầy đủ các tài liệu hướng dẫn thực hiện, kiểm thử, và duy trì công tác đảm bảo hoạt động liên tục đối với hệ thống CNTT.

đ) Thực hiện báo cáo công tác bảo đảm hoạt động liên tục lên TCHQ (Cục CNTT&Thống kê hải quan) để tổng hợp, trình lãnh đạo TCHQ theo định kỳ 6 tháng/lần.

3. Quy định kiểm tra, xây dựng và cập nhật kế hoạch

a) Quy định về kế hoạch kiểm tra và trình Lãnh đạo đơn vị bao gồm:

- Xác định phạm vi và mục tiêu của từng biện pháp kiểm tra.

- Phải lập lịch thực hiện các công tác kiểm tra 6 tháng/lần.

Nội dung kiểm tra:

a1. Kiểm tra các kịch bản khác nhau (trong đó thảo luận về các kịch bản khôi phục hoạt động nghiệp vụ sử dụng các gián đoạn mẫu);

a2. Kiểm tra việc khôi phục kỹ thuật (đảm bảo các hệ thống thông tin có thể được khôi phục thực sự);

a3. Hoàn tất các đợt diễn tập (kiểm tra bảo đảm rằng tổ chức, cá nhân, thiết bị, các phương tiện và quá trình có thể đối phó được với các gián đoạn).

a4. Kiểm tra việc khôi phục từ một vị trí khác (chạy các quy trình nghiệp vụ song song với các hoạt động khôi phục ở xa vị trí chính);

a5. Các cuộc kiểm tra phương tiện và dịch vụ của nhà cung cấp (đảm bảo rằng các dịch vụ và sản phẩm được cung cấp từ bên ngoài sẽ tuân theo cam kết trong hợp đồng).

b) Quy định về cập nhật kế hoạch thay đổi

- Cập nhật những thay đổi, quy trình mới bổ sung thay quy trình cũ;

- Hệ thống CNTT có thay đổi về công nghệ hoặc địa điểm;

- Sau khi thực hiện các biện pháp kiểm tra, đánh giá và các đề xuất.

c) Quy định về kế hoạch đào tạo: Xây dựng và ban hành các tài liệu đào tạo cho từng đối tượng cụ thể: cán bộ, công chức, kỹ năng cho cán bộ kỹ thuật và trình độ quản lý.

Điều 27. Quy định an ninh khi khôi phục sự cố và báo cáo

1. Quy định an ninh khi khôi phục sự cố

a) Quy định xây dựng Kế hoạch khôi phục sự cố

- Kế hoạch, quy trình khôi phục sau sự cố đối với hệ thống CNTT tại đơn vị đã được Lãnh đạo đơn vị phê duyệt.

- Xây dựng các tài liệu hướng dẫn thực hiện kế hoạch, kiểm thử kế hoạch, và cập nhật kế hoạch khôi phục sau sự cố đối với hệ thống CNTT.

- Phải tổ chức báo cáo lên Lãnh đạo đơn vị định kỳ 6 tháng một lần về việc thực hiện kế hoạch khôi phục sau sự cố đối với hệ thống CNTT.

b) Quy định đối với việc xem xét và cập nhật kế hoạch

- Xem xét, cập nhật bổ sung kế hoạch khôi phục sau sự cố định kỳ thực hiện một năm/lần. Khi có thay đổi hệ thống CNTT thì xem xét, cập nhật kế hoạch ngay;

- Xây dựng và cập nhật các biện pháp khôi phục sau sự cố đối với các hệ thống mới.

- Ghi nhật ký quá trình cập nhật kế hoạch.

2. Quy định thực hiện báo cáo an ninh, an toàn Hệ thống CNTT Hải quan

a) Các đơn vị thuộc, trực thuộc TCHQ thực hiện báo cáo định kỳ 6 tháng/lần về Tổng cục Hải quan (qua Cục CNTT&Thống kê hải quan) để tổng hợp, trình Lãnh đạo TCHQ và Bộ Tài chính trước 20/6 và 20/12 hàng năm.

b) Trong các trường hợp cần thiết phải thực hiện các biện pháp về an toàn thông tin, khắc phục sự cố hoặc có vướng mắc phát sinh, các đơn vị thuộc, trực thuộc TCHQ sẽ thực hiện báo cáo đột xuất về TCHQ (qua Cục CNTT&Thống kê hải quan) để tổng hợp, trình Lãnh đạo TCHQ.

c) Mẫu báo cáo: quy định tại Phụ lục I kèm theo quy chế này.

CHƯƠNG IV
ĐẢM BẢO AN NINH, AN TOÀN CHO TÀI LIỆU, QUẢN LÝ THAY ĐỔI, CẬP NHẬT BẢN VÁ, BẢO TRÌ HỆ THỐNG CNTT HẢI QUAN

Điều 28. Quy định bảo đảm an ninh, an toàn cho tài liệu CNTT

1. Trách nhiệm Cục CNTT&Thống kê hải quan

Lưu giữ theo tiêu chuẩn bí mật Nhà nước của ngành Tài chính quy định tại Thông tư 56/2013/BCA-A81 ngày 13/11/2013 V/v Quy định bí mật Nhà nước của Tài chính, và Tài liệu nghiệp vụ của ngành Hải quan:

a) Mã nguồn, thiết kế chi tiết các phần mềm ứng dụng phục vụ công tác của ngành Hải quan.

b) Tài liệu mô tả chi tiết hệ thống mạng, hệ thống an ninh thông tin hải quan (bao gồm thiết kế thi công, sơ đồ kết nối và các thông số kỹ thuật) lưu giữ đầy đủ.

c) Báo cáo chi tiết lỗ hổng bảo mật hệ thống mạng, máy chủ, cơ sở dữ liệu và các ứng dụng hoạt động trên hệ thống mạng của ngành Hải quan.

d) Mật khẩu, các phương tiện xác thực đối tượng truy cập và các hệ thống thông tin của ngành Hải quan (ngoại trừ các hệ thống phục vụ công tác giới thiệu, đào tạo và thử nghiệm).

e) Tài liệu nghiệp vụ về các file dữ liệu chuẩn (CSF), tiêu chí quản lý rủi ro, danh mục rủi ro về giá v.v... .

2. Trách nhiệm các đơn vị thuộc, trực thuộc TCHQ

a) Lưu giữ các tài liệu quy định tại mục (28.1) do đơn vị chủ trì thiết kế, triển khai tại đơn vị.

b) Kiến nghị, đề xuất bảo vệ tài liệu mới về TCHQ (Cục CNTT&Thống kê hải quan).

Điều 29. Quản lý thay đổi

1. Quản lý thay đổi đối với ứng dụng

a) Xác định những nội dung thay đổi của ứng dụng.

b) Lập kế hoạch kiểm tra những thay đổi cửa ứng dụng; đánh giá ảnh hưởng của những thay đổi đối với công việc hiện tại.

c) Thủ tục chấp nhận thay đổi: nâng cấp ứng dụng và cơ sở dữ liệu;

d) Trước khi nâng cấp thực hiện lưu trữ dữ liệu, chương trình.

e) Thực hiện kiểm thử chương trình, dữ liệu (dùng mật khẩu khác với mật khẩu ứng dụng đang triển khai).

f) Triển khai chính thức sau nâng cấp chương trình và dữ liệu.

2. Quản lý thay đổi đối với Hệ điều hành, Cơ sở dữ liệu, phần mềm lớp giữa

a) Thực hiện kiểm thử đối với phiên bản, bản vá Hệ điều hành, cơ sở dữ liệu, phần mềm lớp giữa.

b) Triển khai chính thức phiên bản, bản vá Hệ điều hành, cơ sở dữ liệu, phần mềm lớp giữa.

c) Thay đổi mật khẩu quản trị đối với mỗi lần nâng cấp, thay thế hệ điều hành, Cơ sở dữ liệu, phần mềm lớp giữa.

3. Quản lý thay đổi đối với Trang thiết bị CNTT, ANTT

a) Xác định những nội dung thay đổi đối với trang thiết bị CNTT, ANTT;

b) Triển khai, vận hành thử nghiệm thiết vị CNTT, ANTT khi thay thế.

c) Triển khai chính thức.

Điều 30: Quy định an ninh an toàn khi bảo trì, cập nhật bản vá

1. Trách nhiệm quản lý, kiểm tra, bảo trì, cập nhật bản vá

a) Cục CNTT&Thống kê hải quan: Quản lý toàn bộ các phần mềm, bản vá phần mềm.

Thực hiện kiểm tra, bảo trì, cập nhật bản vá đối với các Hệ thống CNTT Hải quan triển khai tại các DC và DR; Cổng TTĐT Hải quan.

b) Cục Hải quan các tỉnh, thành phố thực hiện kiểm tra, bảo trì, cập nhật bản vá đối với các Hệ thống CNTT Hải quan triển khai tại TTDL&CNTT, Phòng máy chủ tại Cục, Chi cục hải quan trực thuộc; trang/cổng thông tin điện tử của đơn vị quản lý.

c) Các đơn vị hải quan thuộc cơ quan TCHQ kiểm tra, cập nhật bản vá đối với ứng dụng CNTT, trang/cổng thông tin do đơn vị quản lý.

2. Quy định bảo trì hệ thống, thiết bị CNTT

a) Bảo trì hệ thống mạng; trang thiết bị CNTT

- Định kỳ (3-6)tháng/lần thực hiện kiểm tra, bảo dưỡng các trang thiết bị CNTT; năm/lần với thiết bị mạng.

- Nội dung bảo trì thực hiện theo yêu cầu của nhà sản xuất.

- Năm/lần kiểm tra, nâng cấp kỹ thuật đối với các trang thiết bị CNTT.

- Ghi nhật ký quá trình bảo trì; hoạt động của thiết bị.

b) Bảo trì phần mềm thương mại

- Kiểm tra thường xuyên hoạt động của các phần mềm thương mại (VD: Windows; Oracle; SQL Server v.v...).

- Cập nhật đủ các bản vá mới nhất (cung cấp từ chính hãng hoặc nơi cấp tin cậy).

- Kiểm thử các bản nâng cấp, bản vá, đánh giá trước khi triển khai chính thức.

c) Bảo trì ứng dụng

- Phần mềm ứng dụng phải được nhà cung cấp bảo hành theo thỏa thuận.

- Phần mềm ứng dụng phải được bảo trì thường xuyên, sau bảo hành.

- Hàng năm đều rà soát lại chức năng chương trình, phần mềm ứng dụng được nâng cấp để bảo đảm đủ chức năng, yêu cầu kỹ thuật để đáp ứng các yêu cầu quản lý, nghiệp vụ.

- Nội dung bảo trì ứng dụng thực hiện theo tài liệu hướng dẫn.

3. Quy định cập nhật bản nâng cấp, bản vá lỗ hổng bảo mật

a) Cán bộ quản trị của các hệ thống thực hiện kiểm tra thường xuyên, cập nhật bản nâng cấp, bản vá mới nhất đối với hệ thống CNTT (mạng, hệ điều hành, tường lửa, phần mềm thương mại, quản trị dữ liệu, phần mềm ứng dụng).

b) Bản nâng cấp và bản vá do chính hãng cung cấp (hoặc từ nguồn cung cấp tin cậy).

c) Trước khi cập nhật bản nâng cấp, bản vá phải thực hiện kiểm thử, bản kiểm thử bảo đảm, không gây ảnh hưởng tới bản chính thức đang vận hành.

d) Cập nhật bản nâng cấp, bản vá theo hướng dẫn kỹ thuật của nhà cung cấp.

4. Loại bỏ phần mềm an toàn

a) Lãnh đạo đơn vị phê duyệt danh sách phần mềm (phần mềm thương mại, phần mềm ứng dụng) sẽ bị loại bỏ;

b) Thực hiện loại bỏ phần mềm an toàn, không thể khôi phục được (đốt, nghiền nát v.v...);

c) Phần mềm quản trị: phiên bản hết hạn sử dụng cần lưu giữ an toàn, phục vụ kiểm tra truy vết khi cần.

CHƯƠNG IV
TỔ CHỨC THỰC HIỆN

Điều 31. Trách nhiệm của các đơn vị

1. Cục CNTT&Thống kê hải quan

a) Tổ chức triển khai Quy chế đối với các Hệ thống CNTT Hải quan, DC, DR, Cổng TTĐT Hải quan.

b) Hỗ trợ các đơn vi thuộc, trực thuộc TCHQ triển khai quy chế này.

c) Xây dựng trình Tổng cục ban hành các quy trình cụ thể, hướng dẫn vận hành từng phần mềm ứng dụng CNTT.

d) Tổ chức các lớp đào tạo, tập huấn, phổ biến đến cán bộ, công chức, viên chức trong toàn ngành về công tác vận hành, bảo đảm an ninh, an toàn hệ thống CNTT ngành Hải quan.

e) Tổ chức kiểm tra, hướng dẫn việc thực hiện quy chế đối với các đơn vị thuộc, trực thuộc Tổng cục Hải quan.

f) Tiếp nhận, tổng hợp các báo cáo về an ninh, an toàn thông tin của các đơn vị thuộc, trực thuộc TCHQ; định kỳ báo cáo Lãnh đạo TCHQ, Cục Tin học và Thống kê Tài chính 6 tháng/lần vào tháng 6 và tháng 12 hàng năm và báo cáo đột xuất những nội dung liên quan đến ANTT cần phải xử lý ngay.

2. Cục Hải quan các tỉnh, thành phố

a) Triển khai quy chế đối với các hệ thống CNTT thuộc phạm vị Cục quản lý (cấp Cục, Chi cục Hải quan).

b) Phối hợp với Cục CNTT&Thống kê hải quan để tuyên truyền, phổ biến quy chế, tổ chức các lớp đào tạo về ANTT.

c) Định kỳ báo cáo về TCHQ (qua Cục CNTT&Thống kê hải quan) công tác ATTT sáu (6) tháng/lần vào tháng 6 và tháng 12 hàng năm và báo cáo đột xuất những nội dung liên quan đến ANTT cần phải xử lý ngay.

3. Các đơn vị Vụ, Cục thuộc cơ quan Tổng cục Hải quan

a) Triển khai quy chế đối với các hệ thống CNTT thông tin; trang/cổng thông tin trong phạm vi đơn vị quản lý;

b) Định kỳ báo cáo về TCHQ (qua Cục CNTT&Thống kê hải quan) công tác ATTT sáu (6) tháng/lần vào tháng 6 và tháng 12 hàng năm và báo cáo đột xuất những nội dung liên quan đến ANTT cần phải xử lý ngay.

4. Vụ tài vụ quản trị

Vụ Tài vụ quản trị phối hợp Cục CNTT & Thống kê Hải quan ưu tiên bố trí kinh phí thực hiện các nhiệm vụ đảm bảo an ninh, an toàn cho các Hệ thống CNTT Hải quan.

5. Thanh tra Tổng cục Hải quan: phối hợp với Cục CNTT&Thống kê hải quan trong việc kiểm tra thực hiện quy chế này.

Điều 32. Điều khoản thi hành

Trong quá trình thực hiện, có khó khăn, vướng mắc hoặc kiến nghị bổ sung, các đơn vị kịp thời báo về Tổng cục Hải quan (Cục CNTT&Thống kê hải quan) để xem xét, giải quyết, kịp thời bổ sung./.

KT. TỔNG CỤC TRƯỞNG
PHÓ TỔNG CỤC TRƯỞNG

Nguyễn Công Bình

PHỤ LỤC
CÁC MẪU BÁO CÁO

MẪU SỐ 01
BÁO CÁO ĐỊNH KỲ
(Ban hành kèm theo Quy chế số ……ngày …….tháng…….năm 2014 của Tổng cục trưởng Tổng cục hải quan)

TỔNG CỤC HẢI QUAN

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

ĐƠN VỊ:.....

BÁO CÁO ĐỊNH KỲ
Kính gửi: Tổng cục hải quan

Báo cáo định kỳ	6 Tháng ☐	Năm ☐
	Từ tháng…đến tháng…	…..

I.Tình hình hoạt động:
- Tình hình chung
- Các hoạt động, công việc mới phát sinh
- Báo cáo sự cố

II. Kiến nghị

....., ngày.....tháng.....năm.....

NGƯỜI LẬP BIỂU **THỦ TRƯỞNG ĐƠN VỊ**

MẪU SỐ 02

BÁO CÁO ĐỘT XUẤT

(Ban hành kèm theo Quy chế số ……ngày ……tháng……năm 2014 của Tổng cục trưởng Tổng cục hải quan)

TỔNG CỤC HẢI QUAN

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập –Tự do – Hạnh phúc

ĐƠN VỊ:……

BÁO CÁO ĐỘT XUẤT

Kính gửi: Tổng cục hải quan

Báo cáo đột xuất	Khi có sự cố	Khi có sự việc phát sinh	Khác
	☐	☐	☐

I.Tình hình hoạt động:

- Báo cáo khi có sự cố: Thực hiện báo cáo khi có sự cố đột xuất không thể xử lý cần xin ý kiến chỉ đạo của Tổng cục hải quan.
- Khi có sự việc phát sinh: Thực hiện báo cáo khi có sự việc mới phát sinh cần xin ý kiến chỉ đạo xử lý.

II. Đề xuất kiến nghị

....., ngày.....tháng.....năm.....

NGƯỜI LẬP BIỂU **THỦ TRƯỞNG ĐƠN VỊ**

MẪU SỐ 03

BIÊN BẢN KIỂM TRA

(Ban hành kèm theo Quy chế số ……ngày …….tháng…….năm 2014 của Tổng cục trưởng Tổng cục hải quan)

TỔNG CỤC HẢI QUAN

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập –Tự do – Hạnh phúc

ĐƠN VỊ:……

BIÊN BẢN KIỂM TRA

I.Căn cứ kiểm tra

Văn bản số…..

II. Thời gian kiểm tra: .... giờ .... ngày ..... tháng .... năm 201....

III. Địa điểm kiểm tra

.....

.....

IV. Thành phần Đoàn kiểm tra

1.....

2.....

3.....

V. Nội dung kiểm tra

.....

.....

.....

.....

VI. Kết quả kiểm tra và nhận xét của các thành viên Đoàn kiểm tra

.....

.....

.....

.....

VII. Nhận xét:

.....

VIII. Ý kiến của đơn vị:

.....

IX. Kết luận của Đoàn (bộ phận) kiểm tra:

.....

.....

.....

Biên bản được lập thành 02 (hai) bản có giá trị như nhau, ... giữ 01 bản, Đoàn kiểm tra giữ 01 bản.

Biên bản kết thúc vào lúc.....giờ.....cùng ngày, đã đọc lại cho các bên cùng nghe và thống nhất nội dung, ký tên vào Biên bản./.

....., ngày.....tháng.....năm.....

NGƯỜI LẬP BIỂU	**THỦ TRƯỞNG ĐƠN VỊ**