BỘ TÀI CHÍNH **TỔNG CỤC HẢI QUAN**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 1048 /QĐ-TCHQ	*Hà Nội, ngày 14 tháng 4 năm 2020*

QUYẾT ĐỊNH
Về việc Ban hành quy chế bảo đảm an toàn, an ninh thông tin mạng Tổng cục Hải quan

TỔNG CỤC TRƯỞNG TỔNG CỤC HẢI QUAN

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Luật An ninh mạng ngày 12 tháng 06 năm 2018;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Nghị định số 142/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về ngăn chặn xung đột thông tin trên mạng;

Căn cứ Quyết định số 65/2015/QĐ-TTg ngày 17/12/2015 của Thủ tướng Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Tổng cục Hải quan trực thuộc Bộ Tài chính;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ ban hành Quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Căn cứ Quyết định số 1622/QĐ-TTg ngày 25 tháng 10 năm 2017 của Thủ tướng Chính phủ về việc phê duyệt Đề án đẩy mạnh hoạt động của mạng lưới ứng cứu sự cố, tăng cường năng lực cho cán bộ, bộ phận chuyên trách ứng cứu sự cố an toàn thông tin mạng trên toàn quốc đến 2020, định hướng đến 2025;

Căn cứ Thông tư số 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;

Căn cứ Thông tư số 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 của Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin;

Căn cứ Quyết định số 2582/QĐ-BKHCN ngày 25 tháng 9 năm 2017 của

Bộ trưởng Bộ Khoa học và Công nghệ về việc công bố Tiêu chuẩn quốc gia TCVN 11930:2017 yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định 201/QĐ-BTC ngày 12/02/2018 của Bộ trưởng Bộ Tài chính ban hành Quy chế An toàn thông tin mạng Bộ Tài chính;

Căn cứ Quyết định 2445/QĐ-BTC ngày 28/12/2018 của Bộ trưởng Bộ Tài chính ban hành Kiến trúc Chính phủ điện tử ngành Tài chính;

Căn cứ Quyết định 2323/QĐ-BTTTT ngày 31/12/2019 của Bộ trưởng Bộ Thông tin và Truyền thông ban hành Khung Kiến trúc Chính phủ điện tử Việt Nam, phiên bản 2.0;

Căn cứ Quyết định 1728/QĐ-TCHQ ngày 18/6/2019 của Tổng cục trưởng Tổng cục Hải quan ban hành "Kiến trúc và khung tiêu chuẩn an toàn bảo mật hệ thống công nghệ thông tin ngành Hải quan";

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 toàn, an ninh thông tin mạng Tổng cục Hải quan".

Điều 2. Quyết định này có hiệu lực từ ngày ký, thay thế Quyết định số 2926/QĐ-TCHQ ngày 06/10/2014 của Tổng cục trưởng Tổng cục Hải quan về việc "Ban hành quy chế bảo đảm an ninh, an toàn hệ thống Công nghệ thông tin Hải quan".

Điều 3. Cục trưởng Cục Công nghệ thông tin và Thống kê Hải quan, Thủ trưởng các đơn vị thuộc và trực thuộc Tổng cục Hải quan; cán bộ, công chức, viên chức, người lao động trong ngành Hải quan và tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Đơn vị tại Điều 3;
- Bộ Tài chính (để báo cáo);
- Lưu: VT, CNTT (5b).

KT. TỔNG CỤC TRƯỞNG
PHÓ TỔNG CỤC TRƯỞNG

BỘ TÀI CHÍNH
TỔNG CỤC HẢI QUAN

Nguyễn Dương Thái

BỘ TÀI CHÍNH
TỔNG CỤC HẢI QUAN

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

QUY CHẾ
Bảo đảm an toàn, an ninh thông tin mạng Tổng cục Hải quan

(Ban hành kèm Quyết định số 1048/QĐ-TCHQ ngày 14 tháng 4 năm 2020 của Tổng cục trưởng Tổng cục Hải quan)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh: Quy chế này quy định về bảo đảm an toàn, an ninh thông tin mạng trong các hoạt động của Tổng cục Hải quan và các đơn vị thuộc và trực thuộc Tổng cục Hải quan.

2. Đối tượng áp dụng:

a) Các đơn vị thuộc và trực thuộc Tổng cục Hải quan.

b) Cán bộ, công chức, viên chức, người làm việc theo chế độ hợp đồng lao động (người lao động) trong ngành Hải quan

c) Cơ quan, tổ chức, cá nhân có kết nối vào hệ thống mạng của Tổng cục Hải quan.

d) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ công nghệ thông tin và an toàn thông tin mạng (gọi tắt là đối tác công nghệ thông tin) cho các đơn vị thuộc và trực thuộc Tổng cục Hải quan.

Điều 2. Giải thích từ ngữ

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

1. *An toàn thông tin mạng* là sự bảo vệ thông tin số và các hệ thống thông tin trên mạng tránh bị truy cập, 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.

2. *An ninh thông tin 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.

3. *Hạ tầng kỹ thuật* là tập hợp các thiết bị tính toán, lưu trữ, thiết bị ngoại vi, thiết bị kết nối mạng, thiết bị phụ trợ, đường truyền, mạng nội bộ, mạng diện rộng;

4. *Trang thông tin điện tử* là trang thông tin hoặc tập hợp trang thông tin trên môi trường mạng phục vụ cho việc cung cấp, trao đổi thông tin;

5. *Cổng thông tin điện tử* là điểm truy cập duy nhất của cơ quan, đơn vị trên môi trường mạng, liên kết, tích hợp các kênh thông tin, các dịch vụ và các ứng dụng mà qua đó người dùng có thể khai thác, sử dụng và cá nhân hóa việc hiển thị thông tin;

6. *Mã độc hoặc 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 LAN* là hệ thống mạng nội bộ bao gồm mạng dây và mạng không dây;

8. *Mạng WAN* là hệ thống mạng diện rộng, kết nối các mạng LAN;

9. *Dữ liệu nhạy cảm* là dữ liệu có thông tin mật, thông tin lưu hành nội bộ của đơn vị hoặc do đơn vị quản lý, nếu lộ lọt ra ngoài sẽ gây ảnh hưởng xấu đến danh tiếng, tài chính và hoạt động của đơn vị;

10. *Người dùng* là cán bộ, công chức, viên chức, người lao động được cấp quyền sử dụng trang thiết bị CNTT, hệ thống CNTT theo một vai trò cụ thể để thực hiện các nhiệm vụ của mình trên hệ thống CNTT;

11. *Người quản trị* là cán bộ, công chức, viên chức, người lao động được giao nhiệm vụ quản trị, vận hành hệ thống CNTT (bao gồm trang thiết bị phần cứng, phần mềm hệ thống, phần mềm ứng dụng, cơ sở dữ liệu, hệ thống mạng, hệ thống an toàn bảo mật,...);

12. *Tài khoản công nghệ thông tin* bao gồm tài khoản người dùng, tài khoản quản trị hệ thống; là thông tin duy nhất của người dùng/người quản trị hệ thống (bao gồm tên truy cập – username và mật khẩu – password) dùng để truy cập vào hệ thống CNTT và các thông tin cần thiết khác để xác định danh tính của người dùng/người quản trị;

13. *An toàn, an ninh thông tin mạng*: An toàn thông tin mạng và an ninh thông tin mạng;

14. *CNTT*: Công nghệ thông tin;

15. *Cục CNTT&TK Hải quan*: Cục Công nghệ thông tin & Thống kê Hải quan;

16. *Quyết định 201/QĐ-BTC:* Quyết định 201/QĐ-BTC ngày 12/02/2018 của Bộ trưởng Bộ Tài chính ban hành Quy chế An toàn thông tin mạng Bộ Tài chính.

Điều 3. Nguyên tắc bảo đảm an toàn, an ninh thông tin mạng

1. Bảo đảm an toàn, an ninh thông tin mạng là yêu cầu bắt buộc, thường xuyên, liên tục, có tính xuyên suốt quá trình liên quan đến thông tin và thiết kế,

xây dựng, vận hành, nâng cấp, hủy bỏ hệ thống thông tin. Bảo đảm an toàn, an ninh thông tin mạng tuân thủ các nguyên tắc chung quy định tại Điều 4 Luật An toàn thông tin mạng và Điều 4 Nghị định số 85/2016/NĐ-CP.

2. Các đơn vị thuộc và trực thuộc Tổng cục Hải quan có trách nhiệm bảo đảm an toàn, an ninh thông tin mạng của đơn vị mình; căn cứ quy mô, chức năng, điều kiện thực tế của đơn vị để bố trí nhân sự chuyên trách chịu trách nhiệm bảo đảm an toàn, an ninh thông tin mạng cho phù hợp; xác định rõ quyền hạn, trách nhiệm của Thủ trưởng đơn vị, từng bộ phận, cá nhân trong đơn vị đối với công tác bảo đảm an toàn, an ninh thông tin mạng.

3. Cán bộ, công chức, viên chức và người lao động trong ngành Hải quan có trách nhiệm bảo đảm an toàn, an ninh thông tin mạng trong phạm vi xử lý công việc của mình theo quy định của Nhà nước và của ngành Hải quan.

4. Thông tin mật, thông tin thuộc Danh mục bí mật nhà nước ngành Tài chính (thuộc lĩnh vực Hải quan) phải được bảo vệ theo quy định của Nhà nước, quy định của Bộ Tài chính và ngành Hải quan về công tác bảo vệ bí mật nhà nước và các nội dung tương ứng trong Quy chế này.

5. Xử lý sự cố an toàn thông tin mạng phải phù hợp với trách nhiệm, quyền hạn và bảo đảm lợi ích hợp pháp của cơ quan, đơn vị, cá nhân liên quan và theo quy định của pháp luật.

Điều 4. Các hành vi bị nghiêm cấm

1. Các hành vi bị nghiêm cấm quy định tại Điều 7 Luật An toàn thông tin mạng.

2. Tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập mạng không dây của cá nhân vào mạng nội bộ mà không có sự hướng dẫn hoặc đồng ý của đơn vị quản lý hệ thống thông tin; trên cùng một thiết bị thực hiện đồng thời truy cập vào mạng nội bộ và truy cập Internet bằng thiết bị kết nối Internet của cá nhân (modem quay số, USB 3G/4G, điện thoại di động, máy tính bảng, máy tính xách tay).

3. Tự ý thay đổi, gỡ bỏ biện pháp an toàn thông tin cài đặt trên thiết bị công nghệ thông tin phục vụ công việc; tự ý thay thế, lắp mới, tráo đổi thành phần của máy tính phục vụ công việc.

4. Tạo ra, cài đặt, phát tán phần mềm độc hại gây ảnh hưởng đến hoạt động bình thường của hệ thống thông tin.

5. Cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin; ngăn chặn việc truy cập đến thông tin của cơ quan, cá nhân khác trên môi trường mạng, trừ trường hợp pháp luật cho phép.

6. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của cơ quan, cá nhân khác trên môi trường mạng.

7. Các hành vi khác làm mất an toàn, bí mật thông tin của cơ quan, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

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

Điều 5. Xác định cấp độ và phương án bảo đảm an toàn hệ thống thông tin

1. Việc xác định cấp độ hệ thống thông tin và xây dựng phương án bảo vệ hệ thống thông tin theo cấp độ phục vụ mục đích đánh giá an toàn thông tin và bảo đảm an toàn thông tin cho các hệ thống thông tin. Nguyên tắc bảo đảm an toàn thông tin theo cấp độ và nguyên tắc xác định cấp độ căn cứ trên các nguyên tắc quy định tại Điều 4, Điều 5 Nghị định 85/2016/NĐ-CP.

2. Chủ quản hệ thống thông tin

a) Tổng cục Hải quan là chủ quản hệ thống thông tin đối với các hệ thống do Tổng cục Hải quan quyết định đầu tư dự án xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin; là chủ quản hệ thống thông tin do Tổng cục Hải quan phê duyệt đề cương, dự toán chi tiết; quản lý trực tiếp các hệ thống do Bộ Tài chính ủy quyền theo quy định tại điểm a, khoản 1, Điều 5 Quyết định 201/QĐ-BTC.

Tổng cục Hải quan ủy quyền cho các đơn vị thuộc và trực thuộc Tổng cục Hải quan quản lý trực tiếp các hệ thống do Tổng cục Hải quan làm chủ quản thông qua một trong các văn bản sau: Quyết định phê duyệt dự án, trong đó giao đơn vị làm chủ đầu tư dự án; Quyết định của Tổng cục trưởng Tổng cục Hải quan có nội dung giao đơn vị làm nhiệm vụ quản lý hệ thống; Văn bản ủy quyền theo quy định tại khoản 3 Điều 5 Thông tư số 03/2017/TT-BTTTT.

b) Các đơn vị thuộc và trực thuộc Tổng cục Hải quan là chủ quản hệ thống thông tin do đơn vị quyết định đầu tư dự án xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin; là chủ quản hệ thống thông tin do đơn vị phê duyệt đề cương, dự toán chi tiết; quản lý trực tiếp các hệ thống do Tổng cục Hải quan ủy quyền theo quy định tại điểm a khoản này.

c) Chủ quản hệ thống thông tin (hoặc đơn vị được ủy quyền quản lý trực tiếp hệ thống thông tin) thực hiện trách nhiệm theo quy định tại Điều 20 Nghị định 85/2016/NĐ-CP.

3. Đơn vị vận hành hệ thống thông tin

a) Cục CNTT&TK Hải quan là đơn vị vận hành các hệ thống thông tin Tổng cục Hải quan làm chủ quản và các hệ thống thông tin được triển khai tập trung tại Trung tâm quản lý vận hành Hệ thống CNTT Hải quan do các Cục thuộc Tổng cục Hải quan làm chủ quản.

b) Phòng Công nghệ thông tin hoặc phòng thực hiện chức năng tham mưu về công tác công nghệ thông tin tại các Cục Hải quan và tương đương trực thuộc Tổng cục Hải quan là đơn vị vận hành các hệ thống thông tin do Cục Hải quan và tương đương làm chủ quản hoặc được Tổng cục Hải quan ủy quyền quản lý trực tiếp.

c) Các hệ thống thông tin trước khi đưa vào khai thác, sử dụng phải được giao cho đơn vị quản lý, vận hành. Đơn vị vận hành hệ thống thông tin thực hiện

trách nhiệm theo quy định tại khoản 2, 3, 4, 5 Điều 22 Nghị định 85/2016/NĐ-CP và Điều 6 Thông tư số 03/2017/TT-BTTTT.

4. Đơn vị chuyên trách về an toàn thông tin

a) Cục CNTT&TK Hải quan là đơn vị chuyên trách về an toàn thông tin của Tổng cục Hải quan và các đơn vị thuộc Tổng cục Hải quan.

b) Phòng Công nghệ thông tin hoặc phòng thực hiện chức năng tham mưu về công tác công nghệ thông tin tại các Cục Hải quan và tương đương trực thuộc Tổng cục Hải quan đồng thời là đơn vị chuyên trách về an toàn thông tin của các Cục Hải quan và tương đương.

c) Đơn vị chuyên trách về an toàn thông tin thực hiện trách nhiệm theo quy định tại khoản 1 Điều 21 Nghị định 85/2016/NĐ-CP.

5. Thẩm quyền xác định cấp độ an toàn hệ thống thông tin

a) Đơn vị lập hồ sơ đề xuất cấp độ: Đối với các hệ thống thông tin thuộc các nhiệm vụ, dự án đang trong giai đoạn lập dự án, đơn vị lập dự án lập hồ sơ đề xuất cấp độ; Đối với các hệ thống thông tin thuê dịch vụ, đơn vị chủ trì thuê dịch vụ lập hồ sơ đề xuất cấp độ; Đối với các hệ thống thông tin đang trong giai đoạn triển khai, đơn vị chủ trì triển khai lập hồ sơ đề xuất cấp độ; Đối với các hệ thống thông tin đang vận hành, đơn vị vận hành lập hồ sơ đề xuất cấp độ.

b) Thẩm quyền thẩm định và phê duyệt cấp độ:

- Đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin thực hiện thẩm định, phê duyệt hồ sơ đề xuất cấp độ đối với hệ thống thông tin được đề xuất là cấp độ 1 hoặc cấp độ 2.

- Đối với hệ thống thông tin được đề xuất là cấp độ 3: Đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin cần gửi xin ý kiến chuyên môn của Cục CNTT&TK Hải quan và thực hiện thẩm định hồ sơ đề xuất cấp độ; Chủ quản hệ thống thông tin phê duyệt hồ sơ đề xuất cấp độ.

- Đối với các hệ thống thông tin được đề xuất cấp độ 4, 5: Việc đề xuất cấp độ, thẩm định, phê duyệt cấp độ thực hiện theo quy định tại khoản 2 Điều 6 của Quyết định 201/QĐ-BTC.

6. Căn cứ đề xuất cấp độ

Thực hiện theo quy định tại Điều 7 của Quyết định 201/QĐ-BTC.

7. Phương án bảo đảm an toàn hệ thống thông tin

Thực hiện theo quy định tại Điều 8 của Quyết định 201/QĐ-BTC.

8. Quy trình xác định cấp độ

Thực hiện theo quy định tại Điều 9, 10 của Quyết định 201/QĐ-BTC.

9. Điều chỉnh, bổ sung, thay mới hồ sơ đề xuất cấp độ

Khi thực hiện nâng cấp, mở rộng, thay thế một phần hệ thống thông tin, phải rà soát cấp độ, phương án bảo đảm an toàn hệ thống thông tin của hệ thống

thông tin và thực hiện điều chỉnh, bổ sung hoặc thay mới hồ sơ đề xuất cấp độ trong trường hợp cần thiết.

10. Triển khai phương án bảo đảm an toàn hệ thống thông tin

- Chủ quản hệ thống thông tin hoặc đơn vị được ủy quyền quản lý trực tiếp hệ thống thông tin tổ chức triển khai phương án bảo đảm an toàn hệ thống thông tin sau khi hồ sơ đề xuất cấp độ hoặc phương án bảo đảm an toàn hệ thống thông tin được phê duyệt.

- Đơn vị chuyên trách về an toàn thông tin thuộc chủ quản hệ thống thông tin hoặc đơn vị được ủy quyền quản lý trực tiếp hệ thống thông tin chịu trách nhiệm giám sát việc triển khai các phương án bảo đảm an toàn hệ thống thông tin đã được phê duyệt.

Điều 6. Quản lý tài sản công nghệ thông tin

1. Phân loại tài sản công nghệ thông tin:

a) Tài sản phần cứng (vật lý): là các trang thiết bị phần cứng công nghệ thông tin, phương tiện truyền thông và các trang thiết bị phục vụ cho hoạt động của hệ thống thông tin;

b) Tài sản phần mềm: các phần mềm hệ thống, phần mềm thương mại, phần mềm nội bộ, phần mềm ứng dụng, cơ sở dữ liệu và công cụ phát triển phần mềm;

c) Tài sản thông tin: các thông tin, dữ liệu ở dạng số hóa.

2. Yêu cầu về quản lý tài sản công nghệ thông tin:

a) Giao, gắn trách nhiệm cho cá nhân hoặc tập thể quản lý, sử dụng tài sản công nghệ thông tin.

b) Quy định các quy tắc sử dụng, giữ gìn bảo vệ tài sản công nghệ thông tin trong các trường hợp như: mang ra khỏi cơ quan, trang thiết bị công nghệ thông tin liên quan đến dữ liệu nhạy cảm, thông tin cài đặt và cấu hình.

c) Tài sản phần cứng có lưu trữ dữ liệu nhạy cảm khi thay đổi mục đích sử dụng hoặc thanh lý, đơn vị phải thực hiện các biện pháp xóa, tiêu hủy dữ liệu đó đảm bảo không có khả năng phục hồi. Trường hợp không thể tiêu hủy được dữ liệu, đơn vị phải thực hiện tiêu hủy cấu phần lưu trữ dữ liệu trên trang thiết bị công nghệ thông tin đó.

d) Trang thiết bị công nghệ thông tin có bộ phận lưu trữ dữ liệu hoặc thiết bị lưu trữ dữ liệu khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài hoặc ngừng sử dụng phải tháo bộ phận lưu trữ khỏi thiết bị hoặc xóa thông tin, dữ liệu lưu trữ trên thiết bị (trừ trường hợp để khôi phục dữ liệu).

đ) Các đơn vị có trách nhiệm bảo dưỡng, bảo trì và hướng dẫn cách sử dụng, quản lý, vận hành hệ thống hạ tầng kỹ thuật của mình; chỉ định bộ phận chuyên trách về công nghệ thông tin thực hiện quản lý, vận hành và định kỳ

kiểm tra, sửa chữa, bảo trì thiết bị (bao gồm thiết bị đang hoạt động và thiết bị dự phòng).

Điều 7. Bảo đảm an toàn thông tin trong việc quản lý cán bộ, công chức, viên chức và người lao động

1. Phân công nhiệm vụ:

a) Xác định trách nhiệm trong việc bảo đảm an toàn thông tin mạng của vị trí phân công.

b) Đảm bảo người được phân công làm việc tại các vị trí có tiếp xúc với thông tin, dữ liệu nhạy cảm phải qua bước đánh giá, thẩm tra nhân thân và lý lịch tư pháp.

c) Yêu cầu người được phân công phải cam kết bảo mật thông tin bằng văn bản riêng hoặc cam kết trong hợp đồng làm việc, hợp đồng lao động, bao gồm các điều khoản về trách nhiệm của cá nhân sau khi thôi việc tại đơn vị.

2. Sử dụng nguồn nhân lực:

Các đơn vị có trách nhiệm:

a) Sau khi tuyển dụng, tiếp nhận nhân sự mới, đơn vị phải có trách nhiệm phổ biến cho nhân sự mới các quy định về bảo đảm an toàn, an ninh thông tin tại đơn vị; đối với các vị trí tiếp xúc, quản lý các thông tin, dữ liệu quan trọng hoặc quản trị các hệ thống thông tin quan trọng, đơn vị phải yêu cầu nhân sự mới cam kết bảo mật thông tin bằng văn bản hoặc cam kết trong hợp đồng làm việc, hợp đồng lao động.

b) Có biện pháp quản lý tài khoản người dùng của cán bộ, công chức, viên chức và người lao động trên các hệ thống thông tin quan trọng.

c) Thường xuyên rà soát, kiểm tra quyền truy cập vào các hệ thống thông tin đối với tất cả cán bộ, công chức, viên chức và người lao động đảm bảo quyền truy cập phù hợp với nhiệm vụ được giao.

d) Phải thường xuyên tổ chức quán triệt các quy định về an toàn, an ninh thông tin, nhằm nâng cao nhận thức về trách nhiệm bảo đảm an toàn, an ninh thông tin của từng cá nhân trong đơn vị.

đ) Thực hiện đúng quy trình cấp mới, quản lý và thu hồi tài khoản, phân quyền truy cập các hệ thống thông tin và tất cả các tài sản liên quan đến hệ thống thông tin đối với các cá nhân do đơn vị quản lý.

3. Chấm dứt hoặc thay đổi công việc:

Khi cán bộ, công chức, viên chức và người lao động chấm dứt hoặc thay đổi công việc, cơ quan, đơn vị phải:

a) Xác định rõ trách nhiệm của cán bộ, công chức, viên chức, người lao động và các bên liên quan trong quản lý, sử dụng các tài sản công nghệ thông tin được giao.

b) Lập biên bản bàn giao tài sản công nghệ thông tin.

c) Thay đổi hoặc thu hồi quyền truy cập các hệ thống thông tin.

d) Rà soát, kiểm tra đối chiếu định kỳ giữa bộ phận quản lý nhân sự và bộ phận quản lý cấp phát, thu hồi quyền truy cập hệ thống thông tin để đảm bảo tài khoản người dùng của cán bộ, công chức, viên chức và người lao động đã nghỉ việc được thu hồi.

Điều 8. Bảo đảm an toàn về mặt vật lý và môi trường nơi lắp đặt trang thiết bị công nghệ thông tin

1. Các thiết bị kết nối mạng, thiết bị bảo mật quan trọng như tường lửa (firewall), thiết bị định tuyến (router), hệ thống máy chủ, hệ thống lưu trữ SAN, NAS, ... phải được đặt trong trung tâm dữ liệu/phòng máy chủ và phải được thiết lập cơ chế bảo vệ, theo dõi phát hiện xâm nhập và biện pháp kiểm soát truy cập, kết nối vật lý phù hợp với từng khu vực: máy chủ và hệ thống lưu trữ; tủ mạng và đầu nối; thiết bị nguồn điện và dự phòng điện khẩn cấp; vận hành, kiểm soát, quản trị hệ thống. Đơn vị chủ quản trung tâm dữ liệu/phòng máy chủ có trách nhiệm xây dựng nội quy hoặc hướng dẫn làm việc khu vực này.

2. Trung tâm dữ liệu/phòng máy chủ là khu vực hạn chế tiếp cận. Chỉ những cá nhân có quyền, nhiệm vụ theo quy định của thủ trưởng đơn vị mới được phép vào trung tâm dữ liệu/phòng máy chủ. Việc vào, ra trung tâm dữ liệu/ phòng máy chủ phải được kiểm soát bằng thiết bị bảo vệ (quẹt thẻ, vân tay, nhận dạng sinh trắc học,...).

3. Tiêu chuẩn kỹ thuật của Trung tâm dữ liệu/ phòng máy chủ: tuân thủ Tiêu chuẩn hạ tầng kỹ thuật phòng máy chủ ngành Hải quan tại Quyết định số 1727/QĐ-TCHQ ngày 18/6/2019.

Điều 9. Bảo đảm an toàn thông tin đối với hệ thống mạng máy tính

1. Hệ thống mạng nội bộ (LAN):

a) Phải được thiết kế phân vùng theo chức năng cơ bản, tuân thủ Kiến trúc hạ tầng mạng ngành Hải quan tại Quyết định số 1729/QĐ-TCHQ ngày 18/6/2019.

b) Dữ liệu trao đổi giữa các vùng mạng phải được quản lý, giám sát bởi hệ thống các thiết bị mạng, thiết bị bảo mật.

c) Thiết lập, cấu hình các tính năng theo thiết kế của các trang thiết bị bảo mật mạng; thực hiện các biện pháp, giải pháp để dò tìm và phát hiện kịp thời các điểm yếu, lỗ hổng về mặt kỹ thuật của hệ thống mạng; thường xuyên kiểm tra, phát hiện những kết nối, trang thiết bị, phần mềm cài đặt bất hợp pháp vào mạng.

d) Ngắt kết nối (shutdown hoặc disable) cổng mạng không sử dụng.

đ) Định kỳ sao lưu cấu hình thiết bị kết nối mạng LAN.

e) Không được tiết lộ thiết kế, thông số cấu hình hệ thống mạng LAN cho tổ chức, cá nhân khác khi không được phép.

g) Không được tìm cách truy cập dưới bất cứ hình thức nào vào các khu vực không được phép truy cập.

2. Hệ thống mạng diện rộng (WAN):

a) Phải tuân thủ thiết kế theo Kiến trúc hạ tầng mạng ngành Hải quan tại Quyết định số 1729/QĐ-TCHQ ngày 18/6/2019.

b) Các đơn vị Hải quan sử dụng hệ thống mạng WAN của ngành Hải quan và ngành Tài chính có trách nhiệm bảo đảm an toàn thông tin đối với hệ thống mạng nội bộ và các thiết bị của mình khi thực hiện kết nối vào mạng WAN; Thông báo sự cố hoặc các hành vi phá hoại, xâm nhập về Cục CNTT&TK Hải quan để xử lý.

c) Định kỳ sao lưu cấu hình thiết bị kết nối mạng WAN.

d) Không được tiết lộ thông số cấu hình hệ thống mạng WAN cho tổ chức, cá nhân khác.

đ) Không được tìm cách truy cập dưới bất cứ hình thức nào vào các khu vực không được phép truy cập.

3. Kết nối Internet:

a) Hệ thống thông tin được thiết lập kết nối Internet cho các mục đích:

- Cung cấp thông tin; cung cấp dịch vụ công trực tuyến, các dịch vụ trong phạm vi quy định của pháp luật.

- Kết nối tới hệ thống thông tin của các cơ quan, tổ chức để phục vụ hoạt động nghiệp vụ, trao đổi thông tin, phối hợp cung cấp dịch vụ công trực tuyến.

- Cung cấp cổng truy cập ứng dụng nội bộ cho người dùng từ Internet.

- Cập nhật phiên bản phần mềm, bản vá phần mềm; Cập nhật mẫu mã độc, mẫu tấn công.

b) Cán bộ, công chức, viên chức và người lao động các đơn vị được truy cập Internet tại cơ quan cho các mục đích: Cập nhật thông tin tình hình kinh tế, chính trị, xã hội của Việt Nam và thế giới; Tra cứu văn bản quy phạm pháp luật và các tài liệu, thông tin tham khảo phục vụ công việc; Sử dụng các dịch vụ hành chính công; Giao dịch với các cơ quan, tổ chức liên quan tới công việc được giao; Nghiên cứu, học tập nâng cao trình độ.

c) Quy định cách thức kết nối Internet:

- Các đơn vị phải áp dụng các biện pháp kỹ thuật cần thiết bảo đảm an toàn thông tin trong hoạt động kết nối Internet, tối thiểu đáp ứng các yêu cầu sau: có hệ thống tường lửa và hệ thống bảo vệ truy cập Internet, đáp ứng nhu cầu kết nối đồng thời, hỗ trợ các công nghệ mạng riêng ảo thông dụng và có phần cứng mã hóa tích hợp để tăng tốc độ mã hóa dữ liệu và có khả năng bảo vệ

hệ thống trước các loại tấn công từ chối dịch vụ (DDoS); Lọc bỏ, không cho phép truy cập các trang tin có nghi ngờ chứa mã độc hoặc các nội dung không phù hợp.

- Việc truy cập Internet của cán bộ, công chức, viên chức và người lao động được thực hiện thông qua một hoặc một số cách thức sau: Thiết lập mạng riêng gồm các máy tính chỉ phục vụ truy cập Internet; Thiếp lập mạng không dây chỉ phục vụ truy cập Internet; Truy cập Internet từ máy tính làm việc nhưng được kiểm soát qua hệ thống Proxy đã thiết lập các chính sách chặn, lọc thông tin độc hại; mã độc.

d) Không kết nối Internet cho các trường hợp sau:

- Máy tính sử dụng để đọc, soạn thảo, lưu trữ, in ấn văn bản thuộc bí mật nhà nước;

- Máy tính xử lý thông tin trên hệ thống thông tin cấp độ 4 trở lên;

- Máy tính phục vụ quản trị hệ thống thông tin;

- Toàn bộ máy chủ và thiết bị công nghệ thông tin không phải máy tính ngoại trừ các hệ thống bắt buộc phải có giao tiếp với Internet (các hệ thống phục vụ truy cập Internet; cung cấp giao diện ra Internet của trang tin điện tử, dịch vụ công, thư điện tử; phục vụ cập nhật bản vá hệ điều hành, mẫu mã độc, mẫu điểm yếu, mẫu tấn công).

đ) Truy cập mạng, ứng dụng nội bộ từ Internet phải thực hiện xác thực đa yếu tố hoặc qua mạng riêng ảo VPN.

e) Mạng riêng hoặc mạng không dây chỉ phục vụ truy cập Internet phải được cách ly với mạng làm việc (từ vùng mạng riêng hoặc mạng không dây này không truy cập được vào vùng mạng làm việc).

g) Các hệ thống kỹ thuật đảm bảo an toàn kết nối, truy cập Internet phải được cập nhật mẫu mã độc, cập nhật mẫu tấn công liên tục. Công tác giám sát, vận hành các hệ thống này phải được thực hiện thường xuyên.

Điều 10. Bảo đảm an toàn thông tin khi sử dụng máy tính

1. Cán bộ, công chức, viên chức và người lao động chỉ được sử dụng máy tính vào các hoạt động nghiệp vụ. 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.

2. Không tự tiện thay đổi cấu hình, phần cứng của máy tính cá nhân. Cán bộ, công chức, viên chức và người lao động chỉ cài đặt phần mềm hợp lệ và thuộc danh mục phần mềm được phép sử dụng do cơ quan có thẩm quyền ban hành trên máy tính được đơn vị cấp cho mình; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm khi chưa có sự đồng ý của bộ phận chuyên trách về công nghệ thông tin; thường xuyên cập nhật phần mềm và hệ điều hành.

3. Cài đặt phần mềm xử lý phần mềm độc hại và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm; khi phát hiện bất kỳ dấu hiệu nào liên

quan đến việc bị nhiễm phần mềm độc hại trên máy tính phải tắt máy và báo trực tiếp cho bộ phận chuyên trách về công nghệ thông tin để được xử lý kịp thời.

4. Chỉ truy cập vào các trang/cổng thông tin điện tử, ứng dụng trực tuyến tin cậy và các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình; có trách nhiệm bảo mật tài khoản truy cập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác.

5. Tuân thủ các quy định về việc lưu giữ tài liệu trên máy tính cá nhân, đặc biệt đối với các dữ liệu thuộc danh mục mật, tuyệt mật hoặc tối mật phải tuân thủ quy định về quản lý tài liệu mật.

6. Việc sử dụng thiết bị lưu trữ di động như ổ cứng di động, ổ USB, ...:

- Chỉ sử dụng thiết bị lưu trữ di động cho các hoạt động nghiệp vụ, quản lý khi được sự đồng ý của Lãnh đạo đơn vị.

- Thực hiện các biện pháp bảo đảm an ninh, an toàn cho thiết bị lưu trữ di động như quét mã độc định kỳ, mã hóa dữ liệu.

7. Khóa màn hình máy tính khi rời khỏi bàn làm việc. Đăng xuất khỏi hệ thống, ứng dụng khi ngừng sử dụng. Tắt máy sau mỗi buổi làm việc.

Điều 11. Quản lý tài khoản truy cập

1. Tài khoản người dùng:

a) Mỗi người dùng khi sử dụng hệ thống thông tin phải được cấp và sử dụng tài khoản truy cập với định danh duy nhất gắn với người dùng đó. Trường hợp sử dụng tài khoản dùng chung cho một nhóm người hay một đơn vị phải có cơ chế xác định các cá nhân có trách nhiệm quản lý tài khoản.

b) Tài khoản của người dùng không được cấp quyền quản trị trên máy tính nối mạng. Tài khoản quản trị máy tính chỉ được sử dụng trong trường hợp cài đặt phần mềm trên máy tính. Tài khoản quản trị máy tính để bàn phải do bộ phận công nghệ thông tin của đơn vị nắm giữ. Đối với máy tính xách tay, người dùng phải được hướng dẫn sử dụng đúng cách tài khoản quản trị máy tính và có trách nhiệm thực hiện theo đúng hướng dẫn.

c) Trường hợp người dùng thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ hưu phải thông báo kịp thời cho bộ phận quản lý tài khoản công nghệ thông tin để thực hiện điều chỉnh, thu hồi, hủy bỏ các quyền sử dụng của người dùng đối với hệ thống mạng, ứng dụng. Quy định cụ thể như sau:

- Văn bản quyết định về việc bổ nhiệm chức vụ lãnh đạo, thay đổi vị trí công tác, chuyển công tác, thôi việc, nghỉ hưu phải ghi tên bộ phận chịu trách nhiệm quản lý tài khoản công nghệ thông tin tại phần ghi nơi nhận của văn bản. Trường hợp thay đổi vị trí công tác không sử dụng hình thức văn bản quyết định, đơn vị quản lý người dùng phải thông báo cho bộ phận quản lý tài khoản công nghệ thông tin bằng công văn hoặc theo cách thức quy định trong quy trình quản lý tài khoản công nghệ thông tin áp dụng tại đơn vị.

- Tài khoản công nghệ thông tin phải được điều chỉnh, thu hồi, hủy bỏ trong thời gian không quá 03 ngày làm việc tính từ ngày người dùng chính thức chuyển công tác ra khỏi ngành Hải quan, thôi việc, nghỉ hưu; không quá 05 ngày làm việc trong trường hợp thay đổi vị trí công tác trong nội bộ đơn vị hoặc chuyển công tác tới đơn vị khác thuộc ngành Hải quan.

- Phải có văn bản đề nghị của đơn vị Hải quan (Cục Hải quan và tương đương, Chi cục Hải quan và tương đương) quản lý người dùng trong trường hợp cần duy trì tài khoản của người dùng sau thời điểm người dùng chính thức thay đổi vị trí công tác, chuyển công tác, thôi việc, nghỉ hưu; trong đó nêu rõ lý do, các quyền sử dụng cần duy trì và thời gian duy trì.

2. Tài khoản quản trị hệ thống:

a) Tài khoản quản trị hệ thống (mạng, hệ điều hành, thiết bị kết nối mạng, phần mềm, ứng dụng, cơ sở dữ liệu) phải tách biệt với tài khoản truy cập của người sử dụng thông thường. Tài khoản hệ thống phải được giao đích danh cá nhân làm công tác quản trị. Hạn chế dùng chung tài khoản quản trị.

b) Trường hợp cần thiết để đảm bảo an toàn, an ninh cho hệ thống, phải triển khai hệ thống quản lý tài khoản đặc quyền để thực hiện quản lý, lưu giữ, cấp phát tài khoản quản trị hệ thống.

3. Xác thực tài khoản công nghệ thông tin:

a) Mật khẩu tài khoản công nghệ thông tin dùng để truy cập hoặc sử dụng hoặc quản trị hệ thống thông tin; truy cập thiết bị lưu khóa bí mật phải:

- Có tối thiểu 8 ký tự.

- Gồm tối thiểu 3 trong 4 loại ký tự sau: chữ cái viết hoa (A - Z); chữ cái viết thường (a - z); chữ số (0 - 9); các ký tự khác trên bàn phím máy tính (' ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? /) và dấu cách.

- Không chứa tên tài khoản.

b) Mật khẩu phải được đổi ngay sau khi nhận bàn giao từ người khác hoặc có thông báo về sự cố an toàn thông tin, điểm yếu liên quan đến khả năng lộ mật khẩu; mật khẩu phải được đổi tối thiểu 03 tháng một lần đối với tài khoản của người dùng và 02 tháng một lần đối với tài khoản quản trị hệ thống.

c) Người dùng, người quản trị hệ thống có trách nhiệm bảo vệ thông tin tài khoản được cấp, không tiết lộ mật khẩu hoặc đưa cho người khác phương tiện xác thực tài khoản của mình ngoại trừ các trường hợp: cần xử lý công việc khẩn cấp của đơn vị; cần cung cấp, bàn giao cho đơn vị các thông tin, tài liệu do cá nhân quản lý. Chủ tài khoản phải đổi mật khẩu ngay sau khi kết thúc xử lý các việc này.

4. Khi có yêu cầu khóa quyền truy cập hệ thống thông tin của tài khoản đang hoạt động, lãnh đạo đơn vị Hải quan (Cục Hải quan và tương đương, Chi cục Hải quan và tương đương) đang quản lý người dùng có tài khoản cần khóa phải yêu cầu bằng văn bản gửi đơn vị chủ quản hệ thống thông tin. Đơn vị vận

hành hệ thống thông tin thực hiện việc khóa quyền truy cập của tài khoản khi có chỉ đạo của đơn vị chủ quản hệ thống thông tin. Đơn vị chủ quản hệ thống thông tin có quyền khóa quyền truy cập của tài khoản trong trường hợp tài khoản đó thực hiện các hành vi tấn công hoặc để xảy ra vấn đề mất an toàn, an ninh thông tin.

5. Hệ thống tài khoản công nghệ thông tin phải được rà soát hàng năm, đảm bảo các tài khoản và quyền truy cập hệ thống được cấp phát đúng. Các tài khoản không sử dụng trong thời gian 01 năm phải bị khóa hoặc xóa bỏ (sau khi trao đổi, xác nhận với đơn vị sử dụng).

Điều 12. Quản lý an toàn thông tin mức ứng dụng

1. Yêu cầu về bảo đảm an toàn thông tin phải được đưa vào tất cả các công đoạn thiết kế, xây dựng, triển khai và vận hành, sử dụng, nâng cấp phần mềm, ứng dụng.

2. Phần mềm, ứng dụng phải đáp ứng các yêu cầu sau: cấu hình phần mềm, ứng dụng để xác thực người dùng; giới hạn số lần đăng nhập sai liên tiếp; giới hạn thời gian để chờ đóng phiên kết nối; mã hóa thông tin xác thực trên hệ thống; không khuyến khích việc đăng nhập tự động.

3. Thiết lập, phân quyền truy cập, quản trị, sử dụng tài nguyên khác nhau của phần mềm, ứng dụng với người dùng/nhóm người dùng có chức năng, yêu cầu nghiệp vụ khác nhau; tách biệt cổng giao tiếp quản trị phần mềm ứng dụng với cổng giao tiếp cung cấp dịch vụ; đóng các cổng giao tiếp không sử dụng.

4. Chỉ cho phép sử dụng các giao thức mạng có hỗ trợ chức năng mã hóa thông tin như SSH, SSL, VPN hoặc tương đương khi truy cập, quản trị phần mềm, ứng dụng từ xa trên môi trường mạng; hạn chế truy cập đến mã nguồn của phần mềm, ứng dụng và phải đặt mã nguồn trong môi trường an toàn do bộ phận chuyên trách công nghệ thông tin quản lý.

5. Ghi và lưu giữ bản ghi nhật ký hệ thống của phần mềm, ứng dụng trong khoảng thời gian tối thiểu 03 tháng với những thông tin cơ bản: thời gian, địa chỉ, tài khoản (nếu có), nội dung truy cập và sử dụng phần mềm, ứng dụng; các lỗi phát sinh trong quá trình hoạt động; thông tin đăng nhập khi quản trị.

6. Phần mềm, ứng dụng cần được kiểm tra phát hiện và khắc phục các điểm yếu về an toàn, an ninh thông tin trước khi đưa vào sử dụng và trong quá trình sử dụng.

7. Thực hiện quy trình kiểm soát cài đặt, cập nhật, vá lỗi bảo mật phần mềm, ứng dụng trên các máy chủ, máy tính cá nhân, thiết bị kết nối mạng đang hoạt động thuộc hệ thống mạng nội bộ.

Điều 13. Quản lý an toàn thông tin mức dữ liệu

1. Các đơn vị thuộc và trực thuộc Tổng cục Hải quan phải thực hiện bảo vệ thông tin, dữ liệu liên quan đến hoạt động công vụ, thông tin có nội dung quan trọng, nhạy cảm hoặc không phải là thông tin công khai bằng các biện

pháp như: thiết lập phương án bảo đảm tính bí mật, nguyên vẹn và khả dụng của thông tin, dữ liệu; mã hóa thông tin, dữ liệu khi lưu trữ trên hệ thống/thiết bị lưu trữ dữ liệu di động; sử dụng chữ ký số để xác thực và bảo mật thông tin, dữ liệu.

2. Chủ quản hệ thống thông tin hoặc đơn vị được ủy quyền quản lý trực tiếp hệ thống thông tin triển khai hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng; phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau; thực hiện sao lưu dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

3. Các đơn vị Hải quan (Cục Hải quan và tương đương, Chi cục Hải quan và tương đương, Tổ Đội và tương đương) bố trí máy tính riêng không kết nối mạng, đặt mật khẩu, mã hóa dữ liệu và các biện pháp bảo mật khác bảo đảm an toàn thông tin để soạn thảo, lưu trữ dữ liệu, thông tin và tài liệu quan trọng ở các mức độ mật, tuyệt mật, tối mật.

4. Các đơn vị thuộc và trực thuộc Tổng cục Hải quan phải thường xuyên kiểm tra, giám sát các hoạt động chia sẻ, gửi, nhận thông tin, dữ liệu trong hoạt động nội bộ của mình; khuyến cáo việc chia sẻ, gửi, nhận thông tin trên môi trường mạng cần phải sử dụng mật khẩu để bảo vệ thông tin.

5. Đối với hoạt động trao đổi thông tin, dữ liệu với bên ngoài, tập thể cá nhân thực hiện trao đổi thông tin, dữ liệu ra bên ngoài phải cam kết và có biện pháp bảo mật thông tin, dữ liệu được trao đổi. Giao dịch trực tuyến phải được truyền đầy đủ, đúng địa chỉ, tránh bị sửa đổi, tiết lộ hoặc nhân bản một cách trái phép; sử dụng các cơ chế xác thực mạnh, chữ ký số khi tham gia giao dịch, sử dụng các giao thức truyền thông an toàn.

Điều 14. Phòng chống mã độc

1. Trách nhiệm của các đơn vị liên quan trong công tác phòng chống mã độc:

a) Cục CNTT&TK Hải quan:

- Chủ trì triển khai các giải pháp phòng chống mã độc hại trong ngành Hải quan.

- Chịu trách nhiệm chính trong việc triển khai cài đặt, giám sát phòng chống mã độc, xử lý các sự cố liên quan đến mã độc hại tại Trung tâm dữ liệu (Trung tâm quản lý vận hành hệ thống CNTT Hải quan), Trung tâm dữ liệu dự phòng Tổng cục Hải quan và các đơn vị thuộc Tổng cục Hải quan.

- Chịu trách nhiệm hướng dẫn toàn ngành Hải quan thực hiện các biện pháp xử lý sự cố liên quan đến mã độc hại.

b) Các Cục Hải quan tỉnh, thành phố:

- Chịu trách nhiệm phối hợp với Cục CNTT&TK Hải quan triển khai giải pháp phòng chống mã độc hại.

- Chủ trì triển khai cài đặt, giám sát phòng chống mã độc tại đơn vị mình.

- Báo cáo Tổng cục Hải quan (qua Cục CNTT&TK 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 xử lý các sự cố liên quan đến mã độc hại tại đơn vị mình.

2. Phải triển khai biện pháp, giải pháp phòng chống mã độc cho toàn bộ hệ thống thông tin của đơn vị.

3. Cập nhập thường xuyên về các loại mã độc hại mới, triển khai các hành động phòng ngừa tại đơn vị khi có các nguy cơ về các loại mã độc này.

4. Kiểm tra, diệt mã độc đối với vật mang tin nhận từ bên ngoài trước khi sử dụng.

5. Xây dựng các kế hoạch phục hồi đối với từng hệ thống CNTT trong trường hợp xảy ra các sự cố về mã độc máy tính.

6. Phối hợp với các cơ quan, đơn vị chuyên môn về an toàn thông tin thường xuyên cập nhật thông tin về các loại mã độc hại mới để có các phương án phòng ngừa các nguy cơ về các loại mã độc này gây ra.

7. Thống kê, thông báo các sự cố liên quan đến mã độc máy tính trong cơ quan, đơn vị mình theo các kỳ báo cáo.

Điều 15. Quản lý sao lưu dự phòng (Backup)

Chủ quản hệ thống thông tin hoặc đơn vị được ủy quyền quản lý trực tiếp hệ thống thông tin thực hiện quản lý sao lưu dự phòng bảo đảm an toàn dữ liệu như sau:

1. Lập danh sách hệ thống thông tin theo mức độ quan trọng cần được sao lưu, kèm theo thời gian lưu trữ, định kỳ sao lưu, phương pháp sao lưu và thời gian kiểm tra phục hồi hệ thống từ dữ liệu sao lưu.

2. Dữ liệu của các hệ thống thông tin từ mức độ 2 trở lên phải có phương án tự động sao lưu phù hợp với tần suất thay đổi của dữ liệu và bảo đảm nguyên tắc dữ liệu phát sinh phải được sao lưu trong vòng 24 giờ. Dữ liệu sao lưu phải được lưu trữ ra phương tiện lưu trữ ngoài (như băng từ, đĩa cứng, đĩa quang hoặc phương tiện lưu trữ khác) và cất giữ, bảo quản an toàn tách rời với khu vực lắp đặt hệ thống thông tin nguồn.

3. Đối với hệ thống thông tin từ mức độ 2 trở lên phải kiểm tra, phục hồi dữ liệu sao lưu từ phương tiện lưu trữ ngoài tối thiểu 3 (ba) tháng một lần.

Điều 16. Giám sát và ghi nhật ký hoạt động (Log) của hệ thống thông tin

Chủ quản hệ thống thông tin hoặc đơn vị được ủy quyền quản lý trực tiếp hệ thống thông tin thực hiện giám sát và ghi nhật ký hoạt động của hệ thống thông tin như sau:

1. Thực hiện ghi nhật ký và lưu trữ nhật ký về hoạt động của hệ thống thông tin và người sử dụng, các lỗi phát sinh, các sự cố an toàn thông tin. Dữ liệu nhật ký của các hệ thống thông tin từ mức độ 2 trở lên phải được lưu trữ trực tuyến tối thiểu 3 tháng theo hình thức tập trung và sao lưu tối thiểu một năm.

2. Bảo vệ các chức năng ghi nhật ký và thông tin nhật ký, chống giả mạo và truy cập trái phép; bảo đảm người quản trị hệ thống và người sử dụng không thể xóa hay sửa đổi nhật ký hệ thống ghi lại các hoạt động của chính họ.

3. Thực hiện việc đồng bộ thời gian giữa các hệ thống thông tin.

Chương III
QUẢN LÝ TIẾP NHẬN, PHÁT TRIỂN, DUY TRÌ HỆ THỐNG THÔNG TIN

Điều 17. Yêu cầu về an toàn, bảo mật các hệ thống thông tin

Khi xây dựng mới hoặc nâng cấp hệ thống thông tin, chủ đầu tư chỉ định đơn vị lập dự án (với trường hợp xây dựng mới) hoặc Chủ quản hệ thống thông tin hoặc đơn vị được ủy quyền quản lý trực tiếp hệ thống thông tin (với trường hợp nâng cấp) thực hiện xác định cấp độ hệ thống thông tin theo quy định tại Điều 5 Quyết định này. Đối với hệ thống thông tin từ cấp độ 2 trở lên, đơn vị thực hiện:

1. Xây dựng tài liệu thiết kế, mô tả về các phương án bảo đảm an toàn hệ thống thông tin. Trong đó các yêu cầu về an toàn, bảo mật được xây dựng đồng thời với việc xây dựng các yêu cầu kỹ thuật, nghiệp vụ.

2. Xây dựng phương án kiểm tra, xác minh hệ thống được triển khai tuân thủ theo đúng tài liệu thiết kế và yêu cầu bảo đảm an toàn thông tin trước khi nghiệm thu. Kết quả kiểm tra phải lập thành báo cáo và được cấp có thẩm quyền phê duyệt trước khi đưa vào vận hành chính thức.

Điều 18. Bảo đảm an toàn, an ninh các ứng dụng

Các chương trình ứng dụng nghiệp vụ phải đáp ứng các yêu cầu tối thiểu sau:

1. Kiểm tra tính hợp lệ của dữ liệu nhập vào các ứng dụng, bảo đảm dữ liệu được nhập vào chính xác và hợp lệ.

2. Kiểm tra tính hợp lệ của dữ liệu cần được xử lý tự động trong các ứng dụng nhằm phát hiện thông tin sai lệch do các lỗi trong quá trình xử lý hoặc các hành vi sửa đổi thông tin có chủ ý.

3. Có các biện pháp bảo đảm tính xác thực và bảo vệ sự toàn vẹn của dữ liệu được xử lý trong các ứng dụng.

4. Kiểm tra tính hợp lệ của dữ liệu xuất ra từ các ứng dụng, bảo đảm quá trình xử lý thông tin của các ứng dụng là chính xác và hợp lệ.

5. Mã khóa bí mật của người sử dụng trong các hệ thống thông tin từ mức độ 2 trở lên phải được mã hóa ở lớp ứng dụng.

Điều 19. Quản lý mã hóa

1. Quy định áp dụng và đưa vào sử dụng các biện pháp mã hóa theo quy chuẩn kỹ thuật quốc gia về mã hóa dữ liệu sử dụng trong lĩnh vực tài chính hoặc cơ quan nhà nước hoặc tiêu chuẩn quốc tế đã được công nhận.

2. Có biện pháp quản lý khóa mã hóa để bảo vệ thông tin của tổ chức.

Điều 20. An toàn, bảo mật trong quá trình phát triển phần mềm

1. Chủ quản hệ thống thông tin hoặc đơn vị được ủy quyền quản lý trực tiếp hệ thống thông tin thực hiện quản lý quá trình phát triển phần mềm như sau:

a) Quản lý, kiểm soát mã nguồn chương trình. Việc truy cập, tiếp cận mã nguồn chương trình phải theo đúng chức năng nhiệm vụ hoặc phải được sự phê duyệt của cấp có thẩm quyền;

b) Quản lý, bảo vệ tệp tin cấu hình hệ thống.

2. Chủ quản hệ thống thông tin hoặc đơn vị được ủy quyền quản lý trực tiếp hệ thống thông tin thực hiện lựa chọn, kiểm soát đối với dữ liệu kiểm tra, thử nghiệm. Không sử dụng dữ liệu thật của hệ thống thông tin vận hành chính thức cho hoạt động kiểm thử khi chưa thực hiện các biện pháp che giấu hoặc thay đổi đối với dữ liệu chứa thông tin nghiệp vụ và thông tin bí mật.

Điều 21. Quản lý sự thay đổi hệ thống thông tin

Chủ quản hệ thống thông tin hoặc đơn vị được ủy quyền quản lý trực tiếp hệ thống thông tin thực hiện các biện pháp quản lý và kiểm soát sự thay đổi hệ thống thông tin, tối thiểu bao gồm:

1. Thực hiện ghi chép lại các thay đổi; lập kế hoạch thay đổi; thực hiện kiểm tra, thử nghiệm sự thay đổi, báo cáo kết quả; phê duyệt kế hoạch thay đổi trước khi áp dụng chính thức thay đổi phiên bản phần mềm, cấu hình phần cứng, tham số phần mềm hệ thống, quy trình vận hành. Có phương án dự phòng cho việc phục hồi hệ thống trong trường hợp thực hiện thay đổi không thành công hoặc gặp các sự cố không có khả năng dự tính trước.

2. Kiểm tra, đánh giá tác động để bảo đảm hệ thống thông tin hoạt động ổn định, an toàn trên môi trường mới đối với hệ thống thông tin từ mức độ 2 trở lên khi thay đổi phiên bản hoặc thay đổi hệ Điều hành, cơ sở dữ liệu, phần mềm lớp giữa.

Điều 22. Đánh giá an ninh bảo mật hệ thống thông tin

1. Nội dung đánh giá hệ thống thông tin về an ninh bảo mật phải bao gồm các nội dung sau:

a) Đánh giá về kiến trúc hệ thống để xác định tính phù hợp của các thiết bị lắp đặt với kiến trúc hệ thống tổng thể và yêu cầu về an ninh bảo mật;

b) Kiểm tra cấu hình các thiết bị bảo mật, các hệ thống cấp quyền truy cập tự động, hệ thống quản lý thiết bị đầu cuối, danh sách tài khoản;

c) Kiểm tra thử nghiệm mức độ an toàn mạng (Penetration Test), bắt buộc phải thực hiện đối với các hệ thống thông tin có kết nối và cung cấp thông tin, dịch vụ ra Internet, kết nối với doanh nghiệp và bên thứ ba.

2. Chủ quản hệ thống thông tin hoặc đơn vị được ủy quyền quản lý trực tiếp hệ thống thông tin thực hiện đánh giá an ninh bảo mật đối với hệ thống thông tin từ mức độ 2 trở lên theo các nội dung quy định tại Khoản 1 Điều này trước khi đưa vào vận hành chính thức.

3. Trong quá trình vận hành hệ thống thông tin, Chủ quản hệ thống thông tin hoặc đơn vị được ủy quyền quản lý trực tiếp hệ thống thông tin định kỳ thực hiện đánh giá an ninh bảo mật tối thiểu như sau:

a) Sáu tháng một lần đối với hệ thống thông tin mức độ 5 theo các nội dung tại Khoản 1 Điều này;

b) Một năm một lần đối với các hệ thống thông tin mức độ 3, 4 và các trang thiết bị giao tiếp trực tiếp với môi trường bên ngoài như Internet, kết nối với khách hàng và bên thứ ba theo các nội dung tại Khoản 1 Điều này;

c) Hai năm một lần đối với hệ thống thông tin mức độ 1, 2.

4. Kết quả đánh giá phải được lập thành văn bản báo cáo người đại diện hợp pháp và cấp có thẩm quyền. Đối với các nội dung chưa tuân thủ quy định về an toàn thông tin (nếu có) phải đề xuất biện pháp, kế hoạch, thời hạn xử lý, khắc phục.

Điều 23. Quản lý các điểm yếu về mặt kỹ thuật

1. Chủ quản hệ thống thông tin hoặc đơn vị được ủy quyền quản lý trực tiếp hệ thống thông tin thực hiện các biện pháp đánh giá, quản lý và kiểm soát các điểm yếu về mặt kỹ thuật của các hệ thống thông tin đang sử dụng: ghi chép, quản lý thông tin các thành phần có trong hệ thống có khả năng tồn tại điểm yếu an toàn thông tin (như: thiết bị phần cứng, phần mềm hệ điều hành, ứng dụng, cơ sở dữ liệu, và các thành phần khác (nếu có)).

2. Chủ động phát hiện các điểm yếu về mặt kỹ thuật thông qua các hoạt động:

a) Thường xuyên cập nhật thông tin liên quan đến lỗ hổng, điểm yếu về mặt kỹ thuật;

b) Thực hiện dò quét, phát hiện các mã độc, lỗ hổng, điểm yếu về mặt kỹ thuật của các hệ thống thông tin đang sử dụng định kỳ tối thiểu như sau: (i) Sáu tháng một lần đối với hệ thống thông tin mức độ 4 trở lên hoặc các hệ thống thông tin có kết nối với mạng Internet; (ii) Một năm một lần đối với các hệ thống thông tin còn lại.

3. Đánh giá mức độ tác động, rủi ro của từng lỗ hổng, điểm yếu về mặt kỹ thuật được phát hiện của các hệ thống thông tin đang sử dụng và đưa ra phương án, kế hoạch xử lý.

4. Xây dựng, tổ chức triển khai các giải pháp xử lý, khắc phục và báo cáo kết quả xử lý.

Điều 24. Quản lý bảo trì hệ thống thông tin

Chủ quản hệ thống thông tin hoặc đơn vị được ủy quyền quản lý trực tiếp hệ thống thông tin thực hiện quản lý bảo trì hệ thống thông tin như sau:

1. Ban hành quy định bảo trì hệ thống thông tin ngay sau khi đưa vào hoạt động chính thức. Quy định bảo trì tối thiểu bao gồm các nội dung sau:

a) Phạm vi, các đối tượng được bảo trì;

b) Thời điểm, tần suất bảo trì;

c) Quy trình, kịch bản kỹ thuật để thực hiện bảo trì của từng cấu phần và toàn bộ hệ thống thông tin;

d) Khi thực hiện bảo trì nếu phát hiện, phát sinh sự cố phải báo cáo cấp có thẩm quyền để xử lý;

đ) Phân công và xác định trách nhiệm của bộ phận thực hiện bảo trì và giám sát bảo trì.

2. Thực hiện bảo trì theo quy định tại Khoản 1 Điều này đối với hệ thống thông tin do đơn vị quản lý trực tiếp.

3. Rà soát quy định bảo trì tối thiểu một năm một lần hoặc khi hệ thống thông tin có sự thay đổi.

Chương IV
QUẢN LÝ SẢN PHẨM, DỊCH VỤ CỦA BÊN THỨ BA

Điều 25. Ký kết hợp đồng với bên thứ ba

1. Xác định rõ trách nhiệm, quyền hạn và nghĩa vụ của các bên về an toàn, an ninh công nghệ thông tin khi ký hợp đồng. Hợp đồng với bên thứ ba phải bao gồm các điều khoản và nghĩa vụ về an toàn, an ninh thông tin, cam kết không tiết lộ thông tin, trách nhiệm xử lý, vá lỗ hổng phần mềm, điều khoản xử lý vi phạm và trách nhiệm bồi thường thiệt hại của bên thứ ba do vi phạm của bên thứ ba gây ra.

2. Không được thuê một bên thứ ba thực hiện toàn bộ công việc quản trị (chỉnh sửa cấu hình, quản lý dữ liệu, quản lý nhật ký) đối với các hệ thống thông tin quan trọng về an ninh quốc gia.

Điều 26. Trách nhiệm của các đơn vị thuộc và trực thuộc Tổng cục Hải quan trong quản lý các dịch vụ do bên thứ ba cung cấp

1. Cung cấp, thông báo và yêu cầu bên thứ ba thực hiện các quy định của đơn vị về an toàn bảo mật hệ thống thông tin.

2. Các đơn vị thuộc và trực thuộc Tổng cục Hải quan đầu mối làm việc với đối tác phải lập hồ sơ nhật ký giám sát dịch vụ của đối tác cung cấp, bao gồm tối thiểu các thông tin sau:

- Tên đối tác;

- Dịch vụ cung cấp;

- Ngày thực hiện;

- Các vấn đề về an toàn, an ninh thông tin (sự cố gây gián đoạn, mất hay lộ thông tin, lỗ hổng phần mềm, thời gian khắc phục lỗ hổng…);

- Các thay đổi khác trong dịch vụ (nếu có).

3. Đảm bảo triển khai, duy trì các biện pháp an toàn, an ninh của dịch vụ do bên thứ ba cung cấp theo đúng thỏa thuận.

4. Xác định và ghi rõ các tính năng an toàn, các mức độ bảo mật của dịch vụ và yêu cầu quản lý trong các thỏa thuận về dịch vụ do bên thứ ba cung cấp.

5. Áp dụng các biện pháp giám sát chặt chẽ và giới hạn quyền truy cập của bên thứ ba khi cho phép họ truy cập vào hệ thống thông tin của đơn vị.

6. Giám sát nhân sự của bên thứ ba trong quá trình thực hiện hợp đồng. Khi phát hiện nhân sự bên thứ ba vi phạm quy định về an toàn bảo mật phải thông báo và phối hợp với bên thứ ba áp dụng biện pháp xử lý kịp thời.

7. Thu hồi quyền truy cập hệ thống thông tin đã được cấp cho bên thứ ba, thay đổi các khóa, mã khóa bí mật nhận bàn giao từ bên thứ ba ngay sau khi hoàn thành công việc hoặc kết thúc hợp đồng.

Điều 27. Trách nhiệm của bên thứ ba khi cung cấp dịch vụ công nghệ thông tin

1. Ký và thực hiện cam kết bảo mật thông tin cả trong quá trình triển khai và sau khi hoàn tất hợp đồng.

2. 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 bên ký kết hợp đồng và phải được đơn vị Hải quan chấp thuận. Nhân sự bên thứ ba phải ký cam kết không tiết lộ thông tin quan trọng của bên ký kết hợp đồng.

3. 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.

Chương V
GIÁM SÁT, CẢNH BÁO, ỨNG CỨU SỰ CỐ AN TOÀN THÔNG TIN MẠNG

Điều 28. Giám sát an toàn thông tin mạng

1. Chủ quản hệ thống thông tin chỉ đạo việc giám sát đối với các hệ thống thông tin thuộc phạm vi quản lý; phối hợp với Cục CNTT&TK Hải quan và các đơn vị chuyên môn của quốc gia (như Cục an toàn thông tin – Bộ Thông tin và truyền thông; Cục An ninh mạng – Bộ Công An; Bộ tư lệnh 89 – Bộ Quốc phòng; VNCert; …) giám sát theo quy định.

2. Đối tượng giám sát bắt buộc: Hệ thống thông tin từ cấp độ 3 trở lên.

3. Thời gian giám sát tối thiểu: Giám sát 24 giờ/ngày và 7 ngày/tuần đối với hệ thống cấp độ 4, 5; Giám sát trong giờ làm việc đối với hệ thống cấp độ 3.

4. Nội dung, phương thức, hệ thống kỹ thuật phục vụ công tác giám sát: Thực hiện theo quy định tại Điều 5 Thông tư số 31/2017/TT-BTTTT.

Điều 29. Cảnh báo an toàn thông tin mạng

1. Đơn vị chuyên trách về an toàn thông tin cử 01 lãnh đạo đơn vị chuyên trách an toàn thông tin và 01 cán bộ thuộc đơn vị chuyên trách về an toàn thông tin làm đầu mối tiếp nhận cảnh báo an toàn thông tin trong ngành Hải quan từ Cục CNTT&TK Hải quan, các cơ quan, tổ chức có chức năng cảnh báo an toàn thông tin mạng của Bộ Tài chính, Bộ Thông tin và truyền thông, Bộ Công An, Bộ Quốc Phòng.

Đầu mối tiếp nhận cảnh báo phân tích sơ bộ mức độ ảnh hưởng tới các hệ thống thông tin của đơn vị mình, chuyển tiếp cảnh báo cho các bộ phận liên quan xử lý, tổng hợp và gửi báo cáo kết quả xử lý cho đầu mối tiếp nhận cảnh báo của Cục CNTT&TK Hải quan qua thư điện tử hoặc điện thoại hoặc bằng văn bản trong trường hợp được yêu cầu báo cáo bằng văn bản.

2. Đơn vị chuyên trách về an toàn thông tin có trách nhiệm theo dõi, nắm bắt thông tin trên phương tiện thông tin đại chúng và mạng Internet về các sự kiện mất an toàn thông tin có thể tác động tới đơn vị; Chủ động kiểm tra, rà soát trong nội bộ đơn vị theo các văn bản cảnh báo, hướng dẫn của Tổng cục Hải quan, Bộ Tài chính, Bộ Thông tin và truyền thông, Bộ Công An, Bộ Quốc Phòng, các cơ quan chức năng và các tổ chức về an toàn thông tin; Thiết lập kênh trao đổi thông tin với các đối tác cung cấp thiết bị, phần mềm, kênh truyền, giải pháp an toàn thông tin của đơn vị để nắm bắt kịp thời vấn đề, sự cố có khả năng tác động tới hệ thống thông tin của đơn vị.

Điều 30. Ứng cứu sự cố an toàn thông tin mạng

1. Sự cố an toàn thông tin mạng là việc thông tin số, hệ thống thông tin bị tấn công (tấn công từ chối dịch vụ; tấn công giả mạo; tấn công sử dụng mã độc; truy cập trái phép, chiếm quyền điều khiển; tấn công thay đổi giao diện; tấn công mã hóa phần mềm, dữ liệu, thiết bị; phá hoại thông tin, dữ liệu, phần mềm;

nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu; các hình thức tấn công mạng khác) hoặc bị gây nguy hại, ảnh hưởng tới tính bí mật, tính toàn vẹn, tính sẵn sàng

2. Ban chỉ đạo, đơn vị chuyên trách ứng cứu khẩn cấp sự cố an toàn thông tin mạng:

a) Ban Chỉ đạo ứng cứu sự cố an toàn thông tin mạng Tổng cục Hải quan do Tổng cục trưởng Tổng cục Hải quan quyết định. Ban Chỉ đạo ứng cứu sự cố an toàn thông tin mạng Tổng cục Hải quan thực hiện trách nhiệm theo quy định tại khoản 2 Điều 5 Quyết định số 05/2017/QĐ-TTg.

b) Cục CNTT&TK Hải quan là đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng của Tổng cục Hải quan. Đơn vị chuyên trách về an toàn thông tin mạng tại các đơn vị thuộc, trực thuộc Tổng cục Hải quan đảm nhiệm vai trò chuyên trách về ứng cứu sự cố an toàn thông tin mạng trong phạm vi quản lý công nghệ thông tin của đơn vị. Đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng thực hiện trách nhiệm quy định tại khoản 2 Điều 6 Quyết định số 05/2017/QĐ-TTg.

c) Cục CNTT&TK Hải quan thành lập Đội ứng cứu an toàn thông tin mạng Tổng cục Hải quan và tổ chức ứng cứu sự cố đối với các hệ thống thông tin do Tổng cục Hải quan hoặc Cục CNTT&TK Hải quan là chủ quản, hoặc Cục CNTT&TK Hải quan là đơn vị vận hành. Các đơn vị chuyên trách về ứng cứu sự cố tại các đơn vị thuộc và trực thuộc Tổng cục Hải quan thành lập Đội ứng cứu sự cố thuộc đơn vị.

Đội ứng cứu sự cố có trách nhiệm phối hợp với các bên liên quan phân tích, xử lý sự cố an toàn thông tin mạng đối với các sự cố diễn ra trong phạm vi hệ thống thuộc quản lý của chủ quản hệ thống thông tin hoặc phạm vi hệ thống được Tổng cục Hải quan ủy quyền quản lý trực tiếp.

3. Kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng

a) Các đơn vị thuộc và trực thuộc Tổng cục Hải quan tổ chức xây dựng kế hoạch ứng phó sự cố cho các hệ thống thông tin do đơn vị trực tiếp quản lý theo đề cương tại Phụ lục II Quyết định số 05/2017/QĐ-TTg (bao gồm các điều chỉnh do Bộ Thông tin và Truyền thông ban hành nếu có) và tổ chức triển khai kế hoạch sau khi phê duyệt. Cục CNTT&TK Hải quan, Cục Tài vụ quản trị - Tổng cục Hải quan (đối với các nội dung yêu cầu có kinh phí) xem xét cho ý kiến, tổng hợp thành kế hoạch chung toàn ngành, trình Tổng cục Hải quan phê duyệt.

b) Kế hoạch ứng phó sự cố được rà soát và điều chỉnh hàng năm (nếu cần thiết) trước ngày 31 tháng 10, làm cơ sở để xây dựng kế hoạch bảo đảm an toàn, an ninh thông tin năm tiếp theo.

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

a) Các tổ chức, cá nhân khi phát hiện dấu hiệu tấn công hoặc sự cố an toàn thông tin mạng cần nhanh chóng báo cho đơn vị vận hành hệ thống thông tin, đơn vị chủ quản hệ thống thông tin liên quan, Cục CNTT&TK Hải quan.

Cục CNTT&TK Hải quan có trách nhiệm cập nhật, công khai thông tin liên lạc, đường dây nóng của các đơn vị/bộ phận tiếp nhận thông tin sự cố của Tổng cục Hải quan và của các đơn vị thuộc và trực thuộc Tổng cục Hải quan với các đơn vị liên quan.

b) Khi xảy ra sự cố an toàn thông tin mạng thuộc loại hình tấn công mạng, đơn vị vận hành hệ thống thông tin thực hiện báo cáo theo quy định tại Điểm a Khoản 1 Điều 11 Quyết định 05/2017/QĐ-TTg và Điều 9 Thông tư 20/2017/TT-BTTTT, đồng thời báo cáo Cục CNTT&TK Hải quan để tổng hợp, báo cáo Ban Chỉ đạo ứng cứu sự cố an toàn thông tin mạng Tổng cục Hải quan. Trách nhiệm của các đơn vị khi phát hiện, tiếp nhận xác minh, xử lý ban đầu và phân loại sự cố an toàn thông tin mạng theo quy định tại Điều 12 Quyết định 05/2017/QĐ-TTg và Điều 10 Thông tư số 20/2017/TT-BTTTT.

c) Quy trình ứng cứu sự cố an toàn thông tin mạng theo quy định tại Điều 13, Điều 14 Quyết định 05/2017/QĐ-TTg và Điều 11 Thông tư số 20/2017/TT-BTTTT.

4. Diễn tập ứng cứu sự cố an toàn thông tin mạng

a) Chủ quản hệ thống thông tin tổ chức diễn tập ứng cứu sự cố theo kế hoạch ứng phó sự cố được phê duyệt.

b) Cục CNTT&TK Hải quan chủ trì, phối hợp với các đơn vị thuộc và trực thuộc Tổng cục Hải quan tham gia các cuộc diễn tập quốc gia, quốc tế do Cơ quan điều phối quốc gia, Bộ Thông tin và Truyền thông tổ chức và tổ chức diễn tập ứng cứu sự cố trong phạm vi Tổng cục Hải quan theo tần suất quy định tại điểm b Nhiệm vụ 4 mục II Điều 1 Quyết định số 1622/QĐ-TTg ngày 25/10/2017 của Thủ tướng Chính phủ.

Điều 31. Đào tạo, bồi dưỡng nghiệp vụ, tuyên truyền, phổ biến nâng cao nhận thức về an toàn thông tin mạng

1. Các đơn vị thuộc và trực thuộc Tổng cục Hải quan xác định nhu cầu về đào tạo nguồn nhân lực bảo đảm an toàn thông tin tại đơn vị mình gửi Cục CNTT&TK Hải quan. Cục CNTT&TK Hải quan tổng hợp, xây dựng trình Tổng cục Hải quan phê duyệt kế hoạch dài hạn, kế hoạch hàng năm về đào tạo, bồi dưỡng nghiệp vụ an toàn, an ninh thông tin cho cán bộ, công chức, viên chức và người lao động của Tổng cục Hải quan và thực hiện tổ chức đào tạo theo kế hoạch đã phê duyệt.

2. Các đơn vị trực thuộc Tổng cục Hải quan tổ chức đào tạo, bồi dưỡng nghiệp vụ về an toàn thông tin cho cán bộ công nghệ thông tin, cán bộ chuyên trách an toàn thông tin mạng các đơn vị trực thuộc; đào tạo cơ bản về an toàn thông tin cho cán bộ quản lý, người sử dụng máy tính thuộc đơn vị.

3. Các đơn vị trực thuộc Tổng cục Hải quan phải thường xuyên tổ chức các hoạt động tuyên truyền, phổ biến nâng cao nhận thức về bảo đảm an toàn, an ninh thông tin mạng đến toàn thể bộ cán bộ, công chức, viên chức và người lao động tại đơn vị.

4. Cục CNTT&TK Hải quan xây dựng trình Tổng cục Hải quan kế hoạch tuyên truyền, phổ biến nâng cao nhận thức về an toàn, an ninh thông tin mạng tại khối cơ quan Tổng cục Hải quan và thực hiện các nội dung theo kế hoạch đã được phê duyệt.

Điều 32. Chế độ báo cáo

1. Báo cáo định kỳ:

a) Báo cáo an toàn thông tin định kỳ hàng năm gồm các nội dung quy định tại khoản 3 Điều 17 Thông tư 03/2017/TT-BTTTT .

b) Báo cáo hoạt động giám sát của chủ quản hệ thống thông tin định kỳ 6 tháng theo mẫu tại Phụ lục 2 Thông tư 31/2017/TT-BTTTT .

2. Báo cáo đột xuất: Báo cáo về công tác khắc phục mã độc, lỗ hổng, điểm yếu, triển khai cảnh báo an toàn thông tin và các báo cáo đột xuất khác theo yêu cầu của các cơ quan quản lý nhà nước về an toàn thông tin.

3. Trách nhiệm lập, phê duyệt báo cáo

a) Các đơn vị thuộc và trực thuộc Tổng cục Hải quan chịu trách nhiệm:

- Lập báo cáo an toàn thông tin theo quy định tại điểm a khoản 1 điều này, gửi Cục CNTT&TK Hải quan trước ngày 01 tháng 11 hàng năm để tổng hợp báo cáo Cục Tin học & Thống kê Tài chính.

- Lập báo cáo hoạt động giám sát của chủ quản hệ thống thông tin theo quy định tại điểm b khoản 1 điều này, gửi Cục CNTT&TK Hải quan trước ngày 01 tháng 6 và 01 tháng 12 hàng năm để tổng hợp báo cáo Cục Tin học & Thống kê Tài chính.

- Báo cáo đột xuất theo hướng dẫn của Cục CNTT&TK Hải quan.

b) Cục CNTT&TK Hải quan chịu trách nhiệm tập hợp, tổng hợp báo cáo của các đơn vị, báo cáo các cơ quan quản lý nhà nước về an toàn thông tin.

Chương VI
TỔ CHỨC THỰC HIỆN

Điều 33. Trách nhiệm của các đơn vị thuộc và trực thuộc Tổng cục Hải quan

1. Cục CNTT&TK Hải quan:

a) Thực hiện các trách nhiệm được giao tại Quy chế này.

b) Hướng dẫn triển khai Quy chế này và các quy định liên quan của Nhà nước.

c) Tổ chức triển khai thực hiện Quy chế tại Trung tâm dữ liệu, Trung tâm dữ liệu dự phòng Tổng cục Hải quan và các đơn vị thuộc Tổng cục Hải quan.

d) Xây dựng kế hoạch, báo cáo về an toàn thông tin mạng của Tổng cục Hải quan.

2. Các đơn vị thuộc và trực thuộc Tổng cục Hải quan:

a) Thực hiện trách nhiệm của chủ quản hệ thống thông tin trong trường hợp có hệ thống thông tin thuộc quản lý trực tiếp của đơn vị theo quy định của Quy chế này.

b) Tổ chức triển khai thực hiện Quy chế này tại đơn vị.

c) Thực hiện các báo cáo theo quy định, gửi Cục CNTT&TK Hải quan tổng hợp, báo cáo các cấp có thẩm quyền.

3. Các đơn vị vận hành hệ thống thông tin:

a) Thực hiện trách nhiệm của đơn vị vận hành hệ thống thông tin theo quy định tại Quy chế này và các nhiệm vụ do chủ quản hệ thống thông tin phân công.

b) Chỉ đạo, phân công các bộ phận kỹ thuật thuộc đơn vị mình (quản lý ứng dụng; quản lý dữ liệu; vận hành hệ thống thông tin; triển khai và hỗ trợ kỹ thuật) triển khai công tác bảo đảm an toàn thông tin trong tất cả các công đoạn liên quan đến hệ thống thông tin.

4. Các đơn vị chuyên trách về an toàn thông tin:

a) Thực hiện trách nhiệm của đơn vị chuyên trách về an toàn thông tin theo quy định tại Quy chế này và các nhiệm vụ do chủ quản hệ thống thông tin phân công.

b) Phối hợp chặt chẽ với các bộ phận kỹ thuật thuộc đơn vị vận hành hệ thống thông tin trong việc bảo đảm an toàn thông tin trong tất cả các công đoạn liên quan đến hệ thống thông tin.

5. Cơ quan, tổ chức, cá nhân ngoài ngành Hải quan có liên quan: Tuân thủ Quy chế này, quy định công tác bảo vệ bí mật nhà nước của ngành Hải quan, các cam kết, thỏa thuận với các đơn vị thuộc ngành Hải quan về đảm bảo an toàn thông tin khi cung cấp dịch vụ công nghệ thông tin và thực hiện các hoạt động

trao đổi thông tin với các đơn vị thuộc ngành Hải quan. Trường hợp tham gia sử dụng ứng dụng của ngành Hải quan, phải tuân thủ các yêu cầu, hướng dẫn, quy trình đảm bảo an toàn thông tin cụ thể của ứng dụng.

Điều 34. Trách nhiệm tập thể, cá nhân

1. Thủ trưởng đơn vị thuộc đối tượng áp dụng của Quy chế này có trách nhiệm: Phổ biến tới từng cán bộ, công chức, viên chức và người lao động của đơn vị; thường xuyên kiểm tra việc thực hiện Quy chế này tại đơn vị; chịu trách nhiệm trước pháp luật và Lãnh đạo Tổng cục Hải quan 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.

2. Cán bộ, công chức, viên chức, người lao động trong ngành Hải quan thuộc đối tượng áp dụng của quy định có trách nhiệm: Tuân thủ Quy chế; thông báo các vấn đề bất thường liên quan tới an toàn thông tin cho đơn vị, bộ phận chuyên trách về an toàn thông tin mạng của đơn vị; chịu trách nhiệm trước pháp luật và Lãnh đạo đơn vị về các vi phạm, thất thoát dữ liệu mật của ngành Hải quan do không tuân thủ Quy chế.

3. Tập thể, cá nhân vi phạm Quy chế bảo đảm an toàn, an ninh thông tin mạng Tổng cục Hải quan làm ảnh hưởng đến việc thực hiện nhiệm vụ chính trị của ngành Hải quan hoặc gây phương hại đến an ninh quốc gia thì tùy theo tính chất, mức độ của hành vi vi phạm sẽ bị xử lý hành chính, xử lý kỷ luật hoặc truy cứu trách nhiệm hình sự. Nếu gây thiệt hại về tài sản thì phải bồi thường theo quy định của pháp luật.

Điều 35. Kinh phí thực hiện

1. Kinh phí bảo đảm an toàn, an ninh thông tin mạng được lấy từ nguồn ngân sách nhà nước dự toán hàng năm của Tổng cục Hải quan.

2. Căn cứ vào kế hoạch hàng năm, các đơn vị thuộc và trực thuộc Tổng cục Hải quan quan có trách nhiệm xây dựng kế hoạch, đề xuất dự toán cho các hoạt động bảo đảm an toàn, an ninh thông tin mạng gửi Cục CNTT&TK Hải quan để tổng hợp, báo cáo các cấp có thẩm quyền xem xét phê duyệt để thực hiện theo phân cấp.

Điều 36. Công tác kiểm tra

1. Các đơn vị thuộc và trực thuộc Tổng cục Hải quan phải thường xuyên kiểm tra, theo dõi và đánh giá công tác bảo đảm an toàn, an ninh thông tin mạng tại cơ quan, đơn vị mình, coi đây là nhiệm vụ trọng tâm của đơn vị.

2. Giao Cục CNTT&TK Hải quan kiểm tra và báo cáo Lãnh đạo Tổng cục Hải quan việc thực hiện Quy chế này trong toàn ngành.

Điều 37. Trách nhiệm thi hành

1. Thủ trưởng các đơn vị thuộc và trực thuộc Tổng cục Hải quan có trách nhiệm phổ biến, quán triệt đến toàn bộ cán bộ, công chức, viên chức, người lao động trong đơn vị thực hiện các quy định của Quy chế này.

2. Trong quá trình thực hiện, nếu có những vấn đề khó khăn, vướng mắc, các đơn vị phản ánh về Cục CNTT&TK Hải quan để tổng hợp, trình Lãnh đạo Tổng cục xem xét, sửa đổi, bổ sung quy chế./.

KT. TỔNG CỤC TRƯỞNG
PHÓ TỔNG CỤC TRƯỞNG

Nguyễn Dương Thái