

Số: /QĐ-QLCC

Hải Phòng, ngày tháng năm 2024

QUYẾT ĐỊNH

**Ban hành Quy chế bảo đảm an toàn thông tin mạng
tại Ban Quản lý cảng cá, bến cá**

GIÁM ĐỐC BAN QUẢN LÝ CẢNG CÁ, BẾN CÁ

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015; Luật An ninh mạng ngày 12 tháng 6 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 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 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 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 2993/2016/QĐ-UBND ngày 30 tháng 11 năm 2016 của Ủy ban nhân dân thành phố ban hành quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn thành phố Hải Phòng;

Căn cứ Quyết định số 236/QĐ-UBND ngày 30 tháng 01 năm 2023 của Ủy ban nhân dân thành phố về kiện toàn cơ cấu tổ chức của Ban Quản lý cảng cá, bến cá trực thuộc Sở Nông nghiệp và Phát triển nông thôn;

Căn cứ Quyết định số 413/QĐ-STTTT ngày 31 tháng 12 năm 2021 của Sở Thông tin và truyền thông về việc phê duyệt cấp độ an toàn hệ thống thông tin của Sở Nông nghiệp và Phát triển nông thôn;

Căn cứ Quyết định số 276/QĐ-SNN ngày 28 tháng 6 năm 2017 của Sở Nông nghiệp và Phát triển nông thôn về việc ban hành Quy định chức năng, nhiệm vụ, quyền hạn của Ban Quản lý cảng cá, bến cá;

Căn cứ Quyết định số 69/QĐ-SNN ngày 05 tháng 3 năm 2024 của Sở Nông nghiệp và Phát triển nông thôn về việc Ban hành Quy chế bảo đảm an toàn thông tin mạng và an ninh thông tin cho thiết bị camera giám sát;

Xét đề nghị của Trưởng phòng Phòng Hành chính;

QUYẾT ĐỊNH :

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn, an ninh mạng tại Ban Quản lý cảng cá, bến cá.

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

Điều 3. Lãnh đạo Ban Quản lý cảng cá, bến cá; thủ trưởng các phòng, cảng cá và viên chức, người lao động thuộc Ban Quản lý cảng cá, bến cá; các cơ quan, đơn vị, tổ chức, cá nhân có liên quan căn cứ Quyết định thi hành./.

Nơi nhận:

- Sở NN-PTNT; (để b/c)
- Như Điều 3;
- Lưu: VT, PHC.

GIÁM ĐỐC

Đỗ Đức Hưng

QUY CHẾ

Bảo đảm an toàn thông tin mạng tại Ban Quản lý cảng cá, bến cá
(Ban hành kèm theo Quyết định số 11/QĐ-QLCC
ngày 14 tháng 3 năm 2024 của Ban Quản lý cảng cá, bến cá)

Chương I

QUY ĐỊNH CHUNG

Điều 1. Mục đích

1. Nhấn mạnh vào sự cần thiết của việc bảo vệ thông tin và hệ thống mạng khỏi các mối đe dọa và rủi ro, đề ra các giải pháp ứng phó khi gặp sự cố mất an toàn thông tin mạng nhằm đảm bảo một môi trường mạng an toàn và bảo mật.

2. Tạo chuyển biến mạnh mẽ trong nhận thức về an toàn thông tin đối với viên chức, người lao động tại Ban Quản lý cảng cá, bến cá (dưới đây gọi tắt là Ban Quản lý).

Điều 2. Phạm vi điều chỉnh, đối tượng áp dụng

1. Phạm vi điều chỉnh: Quy chế này Quy định về bảo đảm an toàn, an ninh mạng thông tin trong các hoạt động của Ban Quản lý.

2. Đối tượng áp dụng:

a) Áp dụng với tất cả viên chức, người lao động làm việc tại Ban Quản lý theo hợp đồng làm việc, hợp đồng lao động, bao gồm cả người lao động giao kết hợp đồng bằng miệng, người lao động làm việc bán thời gian.

b) Các tổ chức, cá nhân có liên quan kết nối, sử dụng hệ thống thông tin làm việc, cung cấp dịch vụ công nghệ thông tin và an toàn thông tin mạng phục vụ hoạt động tại Ban Quản lý.

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

a) Viên chức, người lao động trực thuộc Ban Quản lý thuộc đối tượng áp dụng Quy chế này có trách nhiệm bảo đảm an toàn, an ninh thông tin mạng; xác định rõ quyền hạn trong phạm vi xử lý công việc của mình theo quy định của pháp luật, hướng dẫn của cơ quan, đơn vị cấp trên có thẩm quyền và các quy định tại Quy chế này.

b) Đảm bảo an toàn thông tin mạng là yêu cầu bắt buộc, thường xuyên, liên tục, có tính xuyên suốt, đồng bộ từ khi thiết kế, xây dựng, vận hành, nâng cấp và hủy bỏ (dừng hoạt động) hệ thống thông tin. Đảm bảo an toàn thông tin mạng phải tuân thủ

các nguyên tắc chung, được quy định tại Điều 4, Luật An toàn thông tin mạng và Điều 4, 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.

c) Việc bảo đảm an toàn hệ thống thông tin được thực hiện một cách tổng thể, đồng bộ, tập trung trong việc đầu tư các giải pháp bảo vệ, có sự dùng chung, chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư thừa, trùng lặp.

d) Viên chức và người lao động thuộc Ban Quản lý có trách nhiệm bảo đảm an toàn, an ninh thông tin trong phạm vi xử lý công việc của mình theo quy định của Ban Quản lý, của Nhà nước và của Sở Nông nghiệp và Phát triển nông thôn.

đ) Xử lý sự cố an toàn thông tin mạng phải phù hợp với trách nhiệm, quyền hạn và đảm bảo lợi ích hợp pháp của Ban Quản lý, các cá nhân liên quan và theo quy định của pháp luật.

Điều 4. Các hành vi bị nghiêm cấm

1. Ngăn chặn việc truyền tải thông tin trên mạng, can thiệp, truy nhập, gây nguy hại, xóa, thay đổi, sao chép và làm sai lệch thông tin trên mạng trái pháp luật.

2. Gây ảnh hưởng, cản trở trái pháp luật tới hoạt động bình thường của hệ thống thông tin hoặc tới khả năng truy nhập hệ thống thông tin của người sử dụng.

3. Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của biện pháp bảo vệ an toàn thông tin mạng của hệ thống thông tin; tấn công, chiếm quyền điều khiển, phá hoại hệ thống thông tin.

4. Phát tán thư rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo.

5. Thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác; lợi dụng sơ hở, điểm yếu của hệ thống thông tin để thu thập, khai thác thông tin cá nhân.

6. Xâm nhập trái pháp luật bí mật mật mã và thông tin đã mã hóa hợp pháp của cơ quan, tổ chức, cá nhân; tiết lộ thông tin về sản phẩm mật mã dân sự, thông tin về khách hàng sử dụng hợp pháp sản phẩm mật mã dân sự; sử dụng, kinh doanh các sản phẩm mật mã dân sự không rõ nguồn gốc.

7. Tự ý đầu nối thiết bị mạng, thiết bị cáp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập không dây của cá nhân vào mạng nội bộ; 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).

8. Các hành vi bị nghiêm cấm được quy định tại Điều 8, Luật An ninh mạng.

Chương II

QUY ĐỊNH CỤ THỂ ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 5. Đảm bảo an toàn thông tin hệ thống mạng

1. Các phòng, cảng cá và cá nhân có trách nhiệm quản lý và bảo quản các trang thiết bị công nghệ thông tin và tài nguyên mạng nội bộ lắp đặt tại phòng làm việc của đơn vị.

2. Khi phát hiện nguy cơ mất an toàn thông tin (cảnh báo từ phần mềm phòng chống mã độc, máy tính hoạt động chậm bất thường, mất dữ liệu), các phòng, cảng cá và cá nhân phải tắt thiết bị công nghệ thông tin, kịp thời báo cáo lãnh đạo trực tiếp quản lý và báo cáo Giám đốc Ban Quản lý (thông qua Phòng Hành chính) để có biện pháp hỗ trợ kịp thời.

Điều 6. Quản lý phòng chống phần mềm độc hại

1. Tất cả các máy tính làm việc tại các phòng, cảng cá phải được trang bị phần mềm phòng chống mã độc. Các phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc khi sao chép, mở các tập tin.

2. Khi gửi văn bản điện tử gửi qua hệ thống thư điện tử phải có định dạng theo Danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước như: (.txt), (.doc), (.odt), (.pdf) và các định dạng khác theo quy định, không được gửi các file thực thi (.com), (.bat), (.exe)...

3. Viên chức và người lao động chủ động tìm hiểu về phòng chống mã độc, các rủi ro do mã độc gây ra; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm khi chưa có sự đồng ý của người có thẩm quyền theo quy định của Ban Quản lý.

4. Tất cả các máy tính của các phòng, cảng cá phải được cấu hình nhằm vô hiệu hóa tính năng tự động thực thi (autoplay) các tập tin trên các thiết bị lưu trữ di động.

5. Phần mềm ứng dụng trước khi được cài đặt, sử dụng phải được kiểm tra xem có phần mềm độc hại tồn tại hay không? Tất cả các tập tin, thư mục phải được quét mã độc trước khi sao chép, sử dụng.

7. Định kỳ hằng năm thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống.

Điều 7. Đảm bảo an toàn thông tin trang thiết bị công nghệ thông tin cá nhân

1. Viên chức, người lao động chịu trách nhiệm về đảm bảo an toàn thông tin thiết bị do mình quản lý và sử dụng.

2. Các thiết bị công nghệ thông tin cá nhân phải được cài đặt và cập nhật thường xuyên phần mềm phòng chống mã độc; thực hiện kiểm tra, rà quét bằng phần mềm

phòng chống mã độc khi sao chép, mở các tập tin hoặc trước khi kết nối các thiết bị lưu trữ dữ liệu di động với máy tính của mình.

3. Cá nhân chịu trách nhiệm và có biện pháp đảm bảo an toàn thông tin, tránh bị lộ lọt dữ liệu khi thực hiện bảo hành, bảo dưỡng, sửa chữa hoặc bảo trì thiết bị do mình quản lý.

4. Khi ngừng sử dụng thiết bị công nghệ thông tin cá nhân, cá nhân phải thực hiện tiêu hủy dữ liệu theo quy định.

Điều 8. Kiểm tra việc tuân thủ quy định về an toàn thông tin và hiệu quả của biện pháp bảo đảm an toàn thông tin

1. Nội dung kiểm tra, đánh giá:

a) Kiểm tra việc xác định cấp độ an toàn hệ thống thông tin và triển khai phương án bảo đảm an toàn thông tin; kiểm tra hiệu quả của các biện pháp bảo đảm an toàn thông tin.

b) Kiểm tra công tác giám sát an toàn thông tin; ứng cứu sự cố an toàn thông tin.

c) Kiểm tra các nội dung khác tại Quy chế này.

Điều 9. Trách nhiệm của bộ phận phụ trách về an toàn thông tin, đơn vị cung cấp dịch vụ

1. Các phòng, cảng cá thực hiện nhiệm vụ bảo đảm an toàn thông tin và ứng cứu sự cố an toàn thông tin mạng theo các quy định tại Quy chế này.

2. Đơn vị cung cấp dịch vụ có trách nhiệm bảo đảm cung cấp đầy đủ các thành phần, chức năng; thiết kế, thiết lập hệ thống đáp ứng các yêu cầu kỹ thuật theo quy định.

3. Quản lý, vận hành, bảo đảm an toàn thông tin cho các thành phần hệ thống thuộc phạm vi quản lý của mình tuân thủ các quy định tại Quy chế này.

Chương III

TỔ CHỨC THỰC HIỆN

Điều 10. Tổ chức triển khai, thực hiện

1. Viên chức, người lao động thuộc Ban Quản lý có trách nhiệm thực hiện Quy chế này.

2. Giám đốc, các Phó Giám đốc Ban Quản lý tổ chức kiểm tra, giám sát, đôn đốc các phòng, cảng cá được giao phụ trách thực hiện Quy chế này.

3. Thủ trưởng các phòng, cảng cá:

a) Triển khai, phổ biến nội dung Quy chế này đến người lao động thuộc thẩm quyền quản lý.

b) Phân công công việc của viên chức, người lao động đảm bảo yêu cầu: không tăng lao động khi chưa phát sinh khối lượng công việc, hoàn thành công việc được giao về số lượng, chất lượng.

4. Phòng Hành chính:

a) Tham mưu, giúp Giám đốc Ban Quản lý thực hiện Quy chế này.

b) Tiếp nhận phản ánh khó khăn, vướng mắc khi thực hiện hoặc khi có sự thay đổi về chế độ chính sách liên quan đến Quy chế này để đề xuất Giám đốc Ban Quản lý xem xét, điều chỉnh, bổ sung.

5. Các đoàn thể trong Ban Quản lý:

a) Tham gia thực hiện Quy chế này.

b) Thực hiện công tác giám sát theo quy định để đảm bảo tính công khai, minh bạch, khách quan.

6. Giải quyết kiến nghị liên quan đến Quy chế này: do Giám đốc Ban Quản lý xem xét, giải quyết hoặc uỷ quyền cho một Phó Giám đốc Ban Quản lý thay mặt Giám đốc Ban Quản lý xem xét, giải quyết.

Điều 11. Sửa đổi, bổ sung Quy chế

1. Quy chế này được sửa đổi, bổ sung trong các trường hợp:

a) Nhà nước có thay đổi về chính sách, pháp luật liên quan đến bảo đảm an toàn thông tin mạng.

b) Hoặc trong quá trình thực hiện có sự thay đổi trong hướng dẫn của các cơ quan chức năng, có thẩm quyền.

c) Căn cứ kiến nghị, đề xuất của người lao động, Giám đốc Ban Quản lý chỉ đạo sửa đổi, bổ sung Quy chế phù hợp với tình hình thực tiễn.

2. Trong quá trình thực hiện, nếu có vướng mắc, các phòng, cảng cá phản ánh về Ban Quản lý (thông qua Phòng Hành chính) để tổng hợp./.