

**BỘ XÂY DỰNG
CỤC HÀNG HẢI VÀ ĐƯỜNG THỦY
VIỆT NAM**

Số: /CHHĐTVN-KHCNMT
V/v tăng cường công tác bảo đảm an toàn
thông tin, an ninh mạng.

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

Hà Nội, ngày tháng 4 năm 2025

Kính gửi:

- Các tổ chức giúp việc Cục trưởng;
- Các đơn vị trực thuộc;
- Công ty TNHH MTV Thông tin điện tử hàng hải Việt Nam.

Hiện nay, tình hình an toàn thông tin có nhiều diễn biến phức tạp, các đối tượng xấu đã sử dụng nhiều thủ đoạn để đánh cắp thông tin, dữ liệu của tổ chức, cá nhân. Vừa qua, một số tài khoản người dùng trong các hệ thống thông tin của Bộ Xây dựng đã bị lộ, lọt trên Internet. Đối với các tài khoản của lãnh đạo, tin tặc có thể lợi dụng quyền hạn của tài khoản để thay đổi các dữ liệu quan trọng, chỉnh sửa, xóa hoặc tạo mới các văn bản giả mạo làm rối loạn công tác quản lý. Các tài khoản lộ lọt cũng gây nguy cơ mất an toàn thông tin, an ninh mạng do tin tặc lợi dụng phát tán mã độc, rà quét các lỗ hổng hệ thống từ đó khai thác, leo thang đặc quyền, chiếm quyền điều khiển hệ thống. Để bảo đảm an toàn thông tin, an ninh mạng, Cục Hàng hải và Đường thủy Việt Nam yêu cầu các đơn vị thực hiện các nội dung sau:

1. Công ty TNHH MTV Thông tin điện tử hàng hải Việt Nam

a) Tăng cường triển khai các biện pháp quản lý, kỹ thuật nhằm bảo đảm an toàn thông tin, an ninh mạng cho hệ thống thông tin phục vụ hoạt động nội bộ và các hệ thống cung cấp dịch vụ công trực tuyến trên mạng của Cục Hàng hải và Đường thủy Việt Nam.

b) Chủ động rà soát các điểm yếu, lỗ hổng bảo mật trên Hệ thống thông tin của Cục Hàng hải và Đường thủy Việt Nam; kịp thời cập nhật các bản vá, cấu hình tăng cường bảo mật cho hệ thống và triển khai các giải pháp phòng ngừa để tránh bị lợi dụng, khai thác để tấn công.

c) Tiếp tục chủ động triển khai 06 giải pháp trọng tâm tăng cường bảo đảm an toàn thông tin, an ninh mạng cho hệ thống thông tin theo hướng dẫn Bộ Thông tin và Truyền thông tại công văn số 2516/BTTTT-CATTT ngày 27/6/2024 (theo yêu cầu của Cục Hàng hải Việt Nam (nay là Cục Hàng hải và Đường thủy Việt Nam) tại công văn số 3504/CHHVN-KHCNMT ngày 29/7/2024).

2. Các đơn vị trực thuộc

a) Tuyên truyền, phổ biến nâng cao nhận thức, trách nhiệm bảo đảm an toàn thông tin, an ninh mạng đến toàn thể công chức, viên chức và người lao động trong đơn vị.

b) Thủ trưởng các đơn vị trực tiếp chỉ đạo công tác bảo đảm an toàn, an ninh mạng và chịu trách nhiệm trước Cục trưởng Cục Hàng hải và Đường thủy

Việt Nam nếu để xảy ra sự cố mất an toàn thông tin mạng tại đơn vị mình.

c) Tăng cường triển khai các biện pháp quản lý, kỹ thuật nhằm bảo đảm an toàn, an ninh mạng cho hệ thống thông tin phục vụ hoạt động nội bộ của đơn vị và các hệ thống cung cấp dịch vụ công trực tuyến trên mạng.

d) Chủ động rà soát các điểm yếu, lỗ hổng bảo mật trên hệ thống thông tin của đơn vị; kịp thời cập nhật các bản vá, cấu hình tăng cường bảo mật cho hệ thống và triển khai các giải pháp phòng ngừa để tránh bị lợi dụng, khai thác để tấn công.

đ) Chủ động rà soát các tài khoản trong các hệ thống thông tin thuộc phạm vi quản lý của đơn vị và các tài khoản được cấp trong các hệ thống thông tin của Cục Hàng hải và Đường thủy Việt Nam, Bộ Xây dựng; thực hiện ngay việc thay đổi mật khẩu tài khoản, không sử dụng mật khẩu mặc định, dễ đoán, định kỳ tối thiểu 03 tháng thay đổi mật khẩu một lần.

e) Khi có sự thay đổi về nhân sự đối với các tài khoản được cấp trong các hệ thống thông tin của Cục Hàng hải và Đường thủy Việt Nam và Bộ Xây dựng, các cơ quan, đơn vị phải cập nhật kịp thời và gửi thông tin (*bao gồm: họ và tên, chức vụ, tên tài khoản, lý do thay đổi, thời điểm thay đổi*) về Cục Hàng hải và Đường thủy Việt Nam (*qua Phòng Khoa học – Công nghệ và Môi trường, Chuyên viên Bùi Ngọc Thi, SĐT: 0374.596.606, Email: thibn@vinamarine.gov.vn*) để thực hiện cập nhật, xử lý theo quy định.

3. Các tổ chức giúp việc Cục trưởng yêu cầu các công chức thực hiện ngay việc thay đổi mật khẩu tài khoản, không sử dụng mật khẩu mặc định, dễ đoán, định kỳ tối thiểu 03 tháng thay đổi mật khẩu một lần. Khi có sự thay đổi về nhân sự đối với các tài khoản được cấp trong các hệ thống thông tin của Cục Hàng hải và Đường thủy Việt Nam và Bộ Xây dựng, các tổ chức giúp việc Cục trưởng phải cập nhật kịp thời và gửi thông tin (*bao gồm: họ và tên, chức vụ, tên tài khoản, lý do thay đổi, thời điểm thay đổi*) về Phòng Khoa học – Công nghệ và Môi trường (*Chuyên viên Bùi Ngọc Thi, SĐT: 0374.596.606, Email: thibn@vinamarine.gov.vn*) để thực hiện cập nhật, xử lý theo quy định.

4. Các đơn vị thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức về an toàn thông tin, an ninh mạng để phát hiện kịp thời các nguy cơ tấn công mạng; và thường xuyên truy cập Trang thông tin điện tử của Cục Hàng hải và Đường thủy Việt Nam (*chuyên mục Chuyển đổi số tại website có địa chỉ <https://vimawa.gov.vn/vi/chuyen-doi-so>*) để cập nhật các cảnh báo, hướng dẫn về an toàn thông tin, an ninh mạng.

5. Các đơn vị thực hiện việc cài đặt, sử dụng các phần mềm (*trong đó có phần mềm diệt virus*) có bản quyền cho các thiết bị máy tính, máy chủ của đơn vị mình để phục vụ nhu cầu công việc.

6. Các đơn vị tổ chức thực hiện bảo trì các sản phẩm của dự án công nghệ thông tin theo quy định tại khoản 26, Điều 1 của Nghị định số 82/2024/NĐ-CP ngày 10/7/2024 của Chính phủ sửa đổi, bổ sung một số điều của Nghị định số 73/2019/NĐ-CP ngày 05 tháng 9 năm 2019 của Chính phủ quy định quản lý đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước.

Trường hợp cần thiết nếu xảy ra sự cố về an toàn thông tin, an ninh mạng

đề nghị liên hệ với Trung tâm Công nghệ thông tin - Bộ Xây dựng, Cục Hàng hải và Đường thủy Việt Nam (*ông Bùi Ngọc Thi chuyên viên Phòng Khoa học - Công nghệ và Môi trường, SĐT: 0374596606, Email: thibn@vinamarine.gov.vn*) và các cơ quan chức năng về an toàn thông tin, an ninh mạng để được hỗ trợ xử lý.

Cục Hàng hải và Đường thủy Việt Nam yêu cầu các đơn vị triển khai thực hiện./.

Nơi nhận:

- Như trên;
- Cục trưởng (*để b/c*);
- Các Phó Cục trưởng;
- Lưu: VT, KHCNMT.

**KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG**

Lê Minh Đạo