KAIRIKI CO., LTD.
7F Suzuyo Nihonbashi Building. 2-1-17 Iwamoto-cho,
Chiyoda-ku, Tokyo, 101-0032 Japan
Tel: 81-3-5846-9515 Fax: 81-3-5846-9516
Mail: info@kairiki-ships.com URL: http://kairiki-ships.com/

February 1st, 2023

ISO27001

KC No. 004

Dear Valued Customers & Business Partners,

USCG Deficiency on Vessel Cyber Risk Management

We have received the latest information regarding Cyber Security Risk Management Deficiencies issued by USGC. This vessel was in San Diego, California, and the detailed items pointed out by USGC are as follows.

- **Vessel failed to install Blocker on USB Ports on all terminals including Main Server on Bridge**
- **Vessel terminal do not have timed session locks/screen saver after extended period of user inactivity**
- **Computer System has generic login**

These deficiencies are considered to be based on the USCG Work Instruction CVC-WI-027(2) as follows:

F. Vessels subject to the ISM Code (U.S. & Foreign Vessels).

1. Basic Cyber Hygiene. The MI/PSCO shall identify when basic cyber hygiene procedures are not in place onboard. These include, but not limited to the following:

a. Poor cyber hygiene

1) Username / Password openly displayed

2) Computer system appears to require a generic login or no login for access

3) Computer system does not appear to automatically log out after extended period of user inactivity

4) Heavy reliance on flash drive/USB media use

USCG Office of Commercial Vessel Compliance (CG-CVC) Mission Management System (MMS) Work Instruction (WI)
Vessel Cyber Risk management Work Instruction CVC-WI-027(2) Org. Date 27OCT20, Rev. Date 18FEB2021

【Recommendations】

1. USB Port Blockers should be used on unused USB ports.
2. Automatic Logout/screen saver should be set up.
3. Windows Login with non-generic password to be used.

Other items on USCG Work Instruction CVC-WI-027(2) should be checked prior to call USA ports.

If you have any concern about cyber security for your vessels, please feel free to contact us.