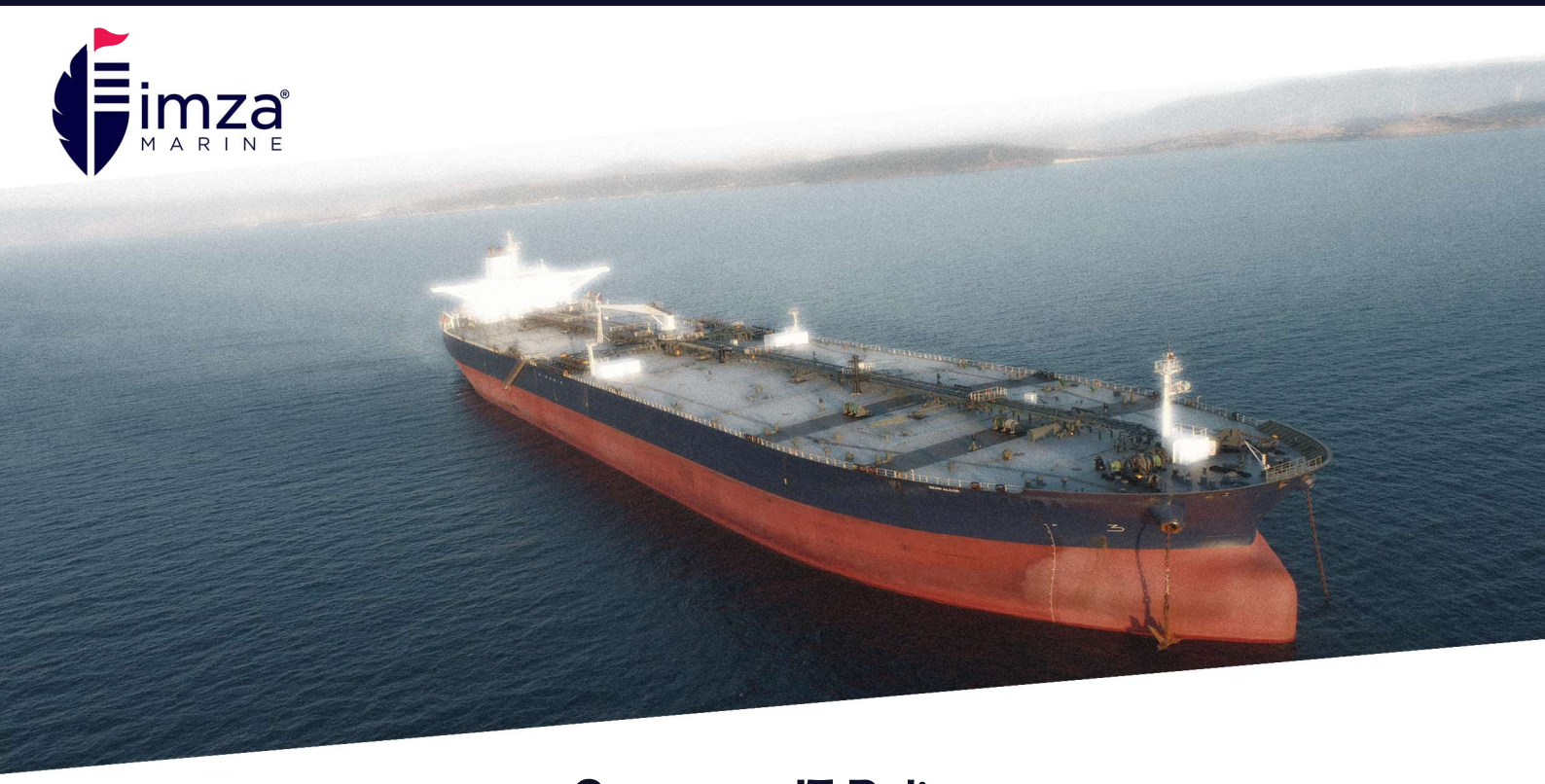

Company IT Policy

Rules Of Conduct For Use Of Internet In The Office

Company/ship systems and electronic communications using those systems, including e-mail, telephone and Internet access, should be used only for business-related purposes. Individuals whohave been given Company/ship e-mail accounts should use only those accounts (and not their personalaccounts) for business functions. Personal e-mail accounts should not be used for business-relatedpurposes unless necessary due to confirmed technical network problems with the Company/shipsystems that prevent your proper use of the Company/ship systems or requested by the Company. Any personal e-mail, telephone and Internet usage, and any other Employee use of Company/ship systems for personal purposes, will be treated the same as business related system usage under this Rules of Conduct and may be resulted by termination of employment contract .

Electronic communications transmitted by or stored on the Company's/ship's systems are subject to all the same Company policies against harassment or threats, discrimination, retaliation, "bullying",defamation and sexual explicitness, pornography as traditional communications. Anything that would be inappropriate to send or state in a non-electronic communication is similarly inappropriate if sent electronically.

Employees **are prohibited** from using the Company's systems to access, transmit, receive, download, store, post, display, print or otherwise disseminate (by e-mail, via the Internet, or through any other formof electronic or voice communication) any unlawful material; or is harmful to the Company's image or business interests; or any material that is discriminatory, harassing or defamatory in nature, that contains ethnic slurs, racial epithets, or that may be perceived as derogatory of others based on race,gender, religion or any other category or classification protected by applicable law.

Using Company systems to send personal electronic communications and **to publish a picture or photograph, video etc. are taken on board or of the Company ships etc. or an assay/picture about the ship or Company** through social or multimedia networking websites (such as Facebook, Twitter, Instagram, LinkedIn, hi5, Second Life, Flickr, YouTube or any similar websites) **is not permitted**.

Employees/crew are responsible of downloading material from the Internet could constitute copyright infringement or violate other intellectual property rights. The unauthorized possession, distribution, uploading, downloading or use of content protected by the copyright, trademark, or other intellectual property laws is prohibited. Employees should not download with or use any of these programs on the Company's/ship's Systems.

Employees/crew should not install software on Company's computer equipment without the approval of the IT department. Any software found on Company systems that has not been approved by the IT department may be removed, along with associated files, without notice to the Employee. Employees are also prohibited from intentionally downloading, storing or executing any security, hacking, spyware, keylogger software, or malware tools on Company networks or systems.

Under this circumstances, every and each employee is responsible of using the Company equipment in accordance with the procedures, and also they are responsible of inappropriate usage out of above mentioned objectives, all those abuses may be resulted by termination of employment contract.

Rules Of Conduct For Use Of Internet On Board

Ship systems and electronic communications using those systems including e-mail, telephone and Internet access, should be used only for business-related purposes.

The primary purpose of usage of the electronic communication equipment and systems on board is to provide the ship communications. In this respect, Company having the full access rights for full intervention on all systems as being fully authorized of logging, reporting, content restriction, partial or total shut down directly or through the Master.

Electronic communications transmitted by or stored on the ship's systems are subject to all the same Company policies against harassment or threats, discrimination, retaliation, "bullying", defamation and sexual explicitness, pornography as traditional communications. Anything that would be inappropriate to send or state in a non-electronic communication is similarly inappropriate if sent electronically.

Crew **are prohibited** from using the ship's systems to access, transmit, receive, download, store, post, display, print or otherwise disseminate (by e-mail, via the Internet, or through any

other form of electronic or voice communication) any unlawful material; or is harmful to the Company's image or business interests; or any material that is discriminatory, harassing or defamatory in nature, that contains ethnic slurs, racial epithets, or that may be perceived as derogatory of others based on race, gender, religion or any other category or classification protected by applicable law.

To publish a picture or photograph, video etc. are taken on board or of the Company ships etc. or an assay/picture about the ship or Company through the social or multimedia networking websites (such as Facebook, Instagram, Twitter, LinkedIn, YouTube or any similar websites) **is strictly prohibited**.

Crew are responsible of downloading material from the Internet could constitute copyright infringement or violate other intellectual property rights. The unauthorized possession, distribution, uploading, downloading or use of content protected by the copyright, trademark, or other intellectual property laws is prohibited. Crewmembers should not download with or use any of these programs on the ship's Systems.

Crewmembers should not install software on ship's computer equipment without approval of the IT department. Any software found on ship's systems that has not been approved by the IT department may be removed, along with associated files, with a notice to the crewmember. Personnel are also prohibited from intentionally downloading, storing or executing any security, hacking, spyware, keylogger software, or malware tools on ship's networks or systems.

Under this circumstances, every and each crewmember is responsible of using the ship's equipment in accordance with the procedures, and also they are responsible of inappropriate usage out of above mentioned objectives, all those breach/abuses may be resulted by termination of employment contract.

Rules Of Conduct For Cyber Security Management

The objective of Cyber Security Management is to protect the company's information assets* (note 1) from all threats, whether internal or external, deliberate or accidental, to ensure operations continuity, minimize damage and maximize return on investments and relevant industry opportunities.

To fulfil these objectives, the management is committed to the following approach:

1) It is the Policy of the Company to ensure that:
    a) Information and Systems identified as vulnerable to Cyber-attacks will be protected from a loss of confidentiality* (note 2), integrity* (note 3) and availability* (note 4).
    b) Regulatory and legislative requirements are to be met.
    c) Cyber Security Contingency Plans have been produced for Support* (note 5).

d) Cyber Security training is available to all staff.
e) All breaches of information security, actual or suspected, will be reported and investigated.

2) Guidance and procedures have been produced to support this policy. These include incident handling, information backup, system access, virus controls, passwords and encryption.

3) The role and responsibility of the IT Manager is to manage information security and to provide advice and guidance on implementation of the Cyber Security Policy.

4) All managers are directly responsible for implementing this Policy within their departments.

5) It is the responsibility of each employee/crew member to adhere to the Cyber Security Policy.

NOTES

1) Information takes many forms and includes data printed or written on paper, stored electronically, transmitted by post or by using electronic means, stored on tape or video, or spoken in conversation.
2) Confidentiality: ensuring that information is accessible only to authorized individuals.
3) Integrity: safeguarding the accuracy and completeness of information and processing methods.
4) Availability: ensuring that authorized users have access to relevant information when required.
5) This will ensure that information and vital services are available to users whenever they need them.