IT Security Policy and Practices

The Company has a policy on information technology security as part of its business ethics and code of conduct. This policy is in place to ensure that the use of technology in business is done in an ethical manner, following governance guidelines. The Company has established and implemented the 'Information Security Management System Policy' to ensure the protection and preservation of sensitive and confidential information through proper implementation of security measures and procedures. Employees ashore as well as aboard ships receive regular cybersecurity awareness training.

Data Privacy Protection

The Company has already formalized its commitment to ensure personal data protection and privacy through its **"Personal Data Protection Policy"**. The purpose of this policy is to provide the appropriate framework for handling personal data and to ensure that there are sufficient security measures in place to protect and secure personal data which the Company is collecting, using, and disclosing in accordance with the PDPA and any related regulations thereof. The Company has also commenced certain specific implementations to fully comply with the law and to prevent any personal data breach or misuse. The Company has appointed a data protection officer primarily to oversee and ensure that the Company's collecting, processing, or disclosing of personal data of its individual stakeholders is following the law and/or other applicable laws and regulations.

Cybersecurity

In response to the evolving landscape of modern maritime operations, we recognize the imperative need to fortify our cybersecurity not only at sea but also within our office environments. As ships become more interconnected and reliant on advanced software, the attention dedicated to cybersecurity becomes paramount to mitigate operational and safety risks. This heightened focus extends across the global shipping industry, where addressing cybersecurity concerns remains a significant challenge for companies worldwide.

Our commitment to enhancing cybersecurity encompasses a multifaceted approach. We continually evaluate and address emerging threats to elevate our overall security posture, cultivating an environment that fosters the organization's work while minimizing the potential for security breaches. The interconnected threads of the global risk environment converge in the realm of cybersecurity, presenting a growing scale and sophistication of risks. Geopolitical trends contribute to this dynamic, as the landscape is susceptible to state-sponsored cyber-attacks that could exacerbate the financially motivated cyber threats prevalent in our industry.

The surge in cyber exposure within companies is a consequence of the rapid proliferation of interconnected devices, the integration of emerging technologies onboard ships, and the utilization of artificial intelligence. To navigate this complex cybersecurity landscape, our industry's primary focus is shifting toward our capacity to respond effectively to the escalating frequency and sophistication of cyber-attacks.

Moreover, our commitment to cybersecurity is underscored by our attainment of ISO/IEC 27001 certification, a globally recognized standard for information security management systems. This certification not only validates our dedication to cybersecurity but also reinforces a holistic approach encompassing the vetting of individuals, establishment of robust policies, and the implementation of cutting-edge technologies.

As we fortify our defenses both at sea and in our offices, we strive to ensure the sustainability and resilience of our company in the face of ever-increasing cyber threats. Our proactive measures, strategic investments, and comprehensive cybersecurity practices position us to adapt and thrive in the digital age while safeguarding the integrity of our operations and the trust of our stakeholders.

Management Information System

As reported in previous years, the computer program implemented by the Company covers all the operations in the head office and links all the vessels in the fleet. This software gives real-time information on vessel operations, costs, etc., and keeps the head office in close contact with the master of each vessel; and assists in effective decision making on all issues. This system has enhanced the company's ability to serve its customers and to provide support to its employees serving onboard the ships. This system is now being upgraded to include additional data collection for new reporting requirements and monitoring of vessels' performance through increased digitalization.

Cyber Incident Response

The Company responds to cyber security hazards and threats through analyzing our cyber security gaps and closing all identified gaps within the organization. We have been working on firewall protection measures to prevent external attacks through applications, using a virtual private network (VPN), and inspecting emails from outside the organization. Furthermore, we have restricted access to unsafe sites, established measures to protect companies from viruses, and backed up organizational data to prevent damage from data theft or other incidents that might create impacts on the Company's data systems in the event of an emergency. In this respect, the Company has also conducted emergency response plan drills to maintain response readiness if an incident were to occur.

The IMO resolution MSC.428(98) on maritime cyber risk management in SMS has already come into effect from 1 January 2021. The resolution states that an approved SMS should consider cyber risk management in accordance with the objectives and functional requirements of the ISM Code. It encourages administrations to ensure that proper risk assessments and measures to protect ships from cyber incidents are included in the SMS. It also requires that these measures be implemented no later than the first annual verification of the Company's DOC after 1 January 2021. We have already completed this on all our vessels.

Although we have not had any cybercrime incidents to date, at PSL we constantly review and maintain our findings that:

- Our present systems incorporated in the office environment and onboard ships are “robust” enough with the understanding that both IT and OT systems may be involved in cyber security incidents.
- The sophistication of cyber threats is rapidly evolving, and it is important that our cyber security systems are able to meet these new and evolving challenges. We work with an external managed detection and response (MDR) provider who assists us with conducting regular vulnerability assessments as well as 24/7 monitoring and threat detection of our key IT infrastructure systems. A vulnerability assessment was also done on a vessel in the fleet. Based on the gap analysis report, we have acted and completed all the recommended measures onboard our ships to increase our cybersecurity posture.
- Additionally, the integrity and vulnerability of our financial and accounting related database is audited by EY once a year.
- We ensure that all network devices and servers have the latest updates installed.
- Although most ships are now connected to the internet, only permitted whitelisted websites can be accessed, minimizing the risk of malware and phishing. The OT systems in machinery spaces and the vital navigation equipment are segregated and not connected to the internet. That minimizes, if not eliminates, the risk due to cyber-attacks onboard ships.
- AIS, ECDIS and Vessel Data Recorders (VDR) etc. are part of the Integrated Bridge System (IBS). Our system setup on-board ensures that such equipment is not directly connected to the internet at any time and hence, no data from such equipment is available or transmitted directly online.

Nevertheless, to reduce vulnerability to both cyber accidents and cyber-attacks, as well as to ensure the safety and efficiency of our operations, the Company has implemented the following additional protocols and practices into its corporate operations and procedures:

- All members of the Company, ranging from senior management ashore to the crew on-board, are involved in the safety and security culture onboard each vessel and in the office environment.
- Incorporating cyber risks into company policies to ensure alignment with the security and safety risk management requirements outlined in the ISPS and ISM Codes.
- Incorporating new related requirements in in-house training programs, relevant onboard procedures, the day-to-day operations of the vessel, and the maintenance of critical cyber systems, if any, that may exist onboard.
- The Company conducts regular security awareness campaigns to educate its employees about the latest cyber threats and how to avoid them. This helps to create a culture of security within the organization.
- The Company ensures that all its systems are regularly updated and patched to protect against known vulnerabilities.
- The Company invests in advanced technology to enhance its cyber security measures. This includes the use of AI and machine learning to detect and prevent cyber threats.
- The Company conducts regular audits and inspections to ensure that all safety and security protocols are being adhered to. This includes checking the effectiveness of the cyber risk management system and making necessary adjustments.