INFORMATION AND CYBER SECURITY MANAGEMENT

This document explains PGS ASA and its subsidiaries' ("PGS") approach to managing Information and Cyber Security Risks in our operations.

A MANAGEMENT APPROACH

A.1 ORGANIZATIONAL STRUCTURE

A.1.1 Board of Directors and Audit Committee

PGS has ensured independent oversight over the Information and Cyber Security Risks that PGS face and its strategy on how these risks are mitigated by PGS. The Board of Directors (the Board) exercises the ultimate authority on PGS' implementation of this strategy and risk management. The Audit Committee being a sub-committee of the Board is following this up closely with PGS management. The majority of the committee members (being the members elected by the shareholders) who serve in the Audit Committee, are independent from PGS and has adequate information and cyber security understanding.

The Audit Committee and Board are briefed on information and cyber security matters in PGS no less than once every year.

A.1.2 Management

PGS has organized its IT activities in a global *Enterprise IT department (EIT)* headed by a *Chief Information Officer (CIO)* reporting to head of the Business Area Technology and Digitalization. The cyber security department is headed by the *Chief Information Security Officer (CISO)* who, inter alia, is responsible for the implementation of PGS' cyber security measures. In addition, PGS has established a data protection workgroup composed by professionals from EIT, Human Resources, Operations, and Legal departments. This workgroup is headed by PGS' *Global Data Protection Officer*.

A.2 MANAGEMENT OF INFORMATION AND CYBER SECURITY RISKS

A.2.1 MITIGATING OUR MATERIAL RISKS

Our most prominent risks are related to cyber crime such as hacking, phishing and ransomware. This may to lead to unavailability of services, data corruption and targeted data theft.

We have established processes for regularly:

- Assessing cyber security risks by using industry standard references
- Presenting results and recommendations from such risk assessments to PGS Management and to the Board
- Testing our security architecture by means of annual internal and external audits, penetration testing and failover testing of critical assets
- Building, maintaining, and monitoring our assets and security architecture
- Logging and actioning security vulnerabilities and improvement opportunities
- Delivering improvements by using Information Technology Infrastructure Library (ITIL) - based processes

PGS has implemented standards and policies covering Information Security which have involved the Board.

A.2.2 AUDITS AND CERTIFICATION

Our main vessel operations have been certified by a third party under the DNV Cyber secure+ program. As part of our Information Security framework, PGS contracts external partners to conduct annual security penetration tests both internally and externally. PGS' Information Security systems are regularly, and at least annually, subject to internal and external audit reviews. Internal and external audit is conducted by certified information and cybersecurity professionals.

A.2.3 AWARENESS

PGS provides specialized training for people particularly exposed to information security risks.

All employees are required to review and confirm their understanding of the key principles of information and cyber security as part of the annual Code of Conduct compliance acknowledgement, and we regularly communicate about cyber security topics via our internal news portal.

A.2.4 OUTSOURCED DATA PROCESSING

In compliance with the EU General Data Protection Regulation (GDPR), Data Processing Agreements (DPAs) have been established with third parties processing personal data on behalf of PGS. These DPAs inter alia address the requirements for establishing, maintaining, and monitoring adequate information security. Our due diligence when sourcing IT services also includes assessing security capabilities, while compliance with international IT security practices are standard requirements.