In undertaking the business continuity planning process, the Company has developed and implemented an Information Security Management System in accordance with the legal regulations of the Republic of Croatia applicable to the organization in the fields of information security, protection and confidentiality of business, contractual and personal data and requirements of the international standard ISO 27001: 2013 in the scope of sustainability and continuity of support processes crucial for the Viktor Lenac Shipyard's operations.

To preserve continuity of the Viktor Lenac Shipyard's operations, it is important to take measures aimed at protecting information assets from all, internal and external, and intentional or accidental, threats to confidentiality, integrity and availability of information.

The Company's Management Board has disclosed the vision, mission and strategy of the organization based on which the Information Security Policy was developed in support of preserving the continuity of the Viktor Lenac Shipyard's operations founded on the following principles:

- Ensuring information confidentiality and protecting information or data from unauthorized access and misuse;
- Maintaining data integrity aimed at ensuring and preserving the validity and accuracy of data;
- Making data and information systems available to stakeholders in accordance with business needs;
- Building relationships and maintaining communication with stakeholders while understanding the context, needs and expectations of stakeholders;
- Carrying out identification, analysis and assessment of information security risks in planned intervals;
- Making decisions and undertaking actions based on the results of information security risk assessments;
- Building awareness and ability of employees for information security through education and training;
- Ensuring compliance with legal, regulatory and contractual requirements, as well as other information security requirements that we have undertaken to comply with by implementing appropriate information security measures;
- Ensuring adequate control and continuous improvement by setting measurable objectives and monitoring performance of the system and applied measures;
- Promptly reporting the threat to information security to the responsible persons for information security management;
- Investigating and analyzing security incidents and initiating appropriate actions to eliminate the causes of threats and reduce risks;
- Developing, maintaining and testing plans for recovery from the consequences of security incidents aimed at maintaining business continuity.

The Company is committed to ensuring the availability of information and the necessary resources to achieve general and individual goals related to information security.

The Company is committed to compliance with all applicable legal and other requirements that the Company has undertaken to comply with in terms of the use of information.

The Management Board of the Company shall ensure that all employees of the Shipyard are acquainted with the Information Security Policy, as well as all external parties that have a role in the Information Security Management System.

All Shipyard employees have been acquainted with this policy and the objectives that flow from it.

The Management Board of the Company shall support proposals to improve the management system at all functions and levels of the organization and by all employees.

The implementation of measures from this policy and the realization of the objectives arising from it is the obligation of all employees.

At least once a year, the Management Board shall evaluate the adequacy of the Information Security Policy and shall update it if necessary.

This document is valid from the date of adoption.

Sandra Uzelac

Member of the Board