INSTITUT IGH, d.d.

INFORMATION SECURITY POLICY

This Policy sets forth the framework for INSTITUT IGH, d.d. Information Security Management System (hereinafter: Institut IGH). The Policy is the principal information security document and its postulates have been incorporated into the Institut IGH information security regulation as well as in other internal Information Security Acts.

The Policy and the inferred internal acts on information security apply to the overall Institut IGH business operations, that is, to all IGH employees, all employees of their business partners and to all locations of Institut IGH business operations.

IGH offers design services, elaboration of studies, technical supervision services, consulting, investigation works, proof of serviceability, laboratory testing and calibration and scientific research work in the field of civil engineering. In order to provide high quality services on time and safe from attacks on information security, Institut IGH is establishing an Information Security Management System (hereinafter: System) whose principal objectives are:

- **Ensuring business continuity and availability of critical systems.** Institut IGH business operations increasingly depend on information systems and data stored in them. Such systems have an impact on the continuity, quality, and timely provision of services as well as on its information security. It is of vital importance that the critical Institut IGH systems are continuously accessible with a guaranteed minimum downtime in case of unpredictable scenarios.
- **Information asset management and risk management** of information systems used or owned by Institut IGH. Owing to permanent changes and advancement in technology, Institut IGH continuously monitors the risks that can impact the confidentiality, integrity and availability of information in the information systems and undertakes the necessary risk mitigation measures of information system use.
- **Minimising the effects** of unwanted and unexpected events by applying information security measures and security measures provided by law.
- **Defining and maintaining the System documentation,** necessary for efficient Institut IGH information security management.
- **Inclusion** of all employees in education programs and permanent awareness of information security.
- **Compliance** with the regulations in the field of data protection.

Institut IGH is fully committed to preserving the confidentiality, integrity and availability of the overall tangible and intangible information assets in all organizational units in order to preserve the reputation, maintain competitive advantage, comply with legal regulations and assumed contractual obligations.

When managing information security risks, Institut IGH considers for each security risk the fulfilment of the principles of confidentiality, integrity and availability in order to assess the threat as objectively and accurately as possible, identify and apply appropriate security measures to mitigate the risk associated with it, and ensure the resilience of information systems to internal and external threats to information security.

Information security requirements are aligned with the organization's strategy and objectives at all levels, and Institut IGH employees are adequately trained and familiar with responsibilities for preserving the confidentiality, integrity and availability of information assets within their scope in accordance with the applicable procedures and instructions of the Information Security Management System.

Proper application of the Information Security Management System can only be ensured through support and involvement of all Institut IGH employees. They must be familiar with this Policy, respective Regulations and procedures. The contents of this Policy must be an integral part of the basic training of new Institut IGH employees.

Every Institut IGH employee is responsible for reporting on a real or presumed case of information security threat.

Institut IGH carries out continuous and systematic activities to protect information assets and systematically monitors those impacts that can have a significant impact or act on information security, paying particular attention to suppliers of products and services used by Institut IGH.

The application of the Policy is subject to internal supervision in accordance with the annual internal control plan and programme. This Policy enters into force on the date of adoption. It is a public document of Institut IGH and is accessible to all interested parties.

In Zagreb, 22 January 2021

Robert Petrosian
President of the Management Board