INFORMATION SECURITY POLICY

Keeping the Information Security a top priority in the business and operational planning the Aqurance top management has approved an Information Security Management System in order to ensure data security, business continuity and minimization of risk of damage by a) preventing security incidents and b) reducing their potential impact.

The goal of this Information Security Policy is to set the framework for protecting the organization's information assets against all internal, external, deliberate or accidental threats.

Aqurance management declares a strong commitment to maintaining standards of information security in line with its business strategy and objectives. Aqurance shall establish, maintain and operate an Information Security Management System to ensure that:

- A framework for establishing information security control objectives and controls is available to protect information against any unauthorized access and to reduce the risk of unacceptable use of any of the AQURANCE information resources.
- A risk assessment approach is adopted with regards to risk management.

- Legislative, business and regulatory requirements, as well as contractual security obligations that are of particular importance to Aqurance are met.
- Business continuity plans are developed, maintained and tested.
- Information security education and training is available for all employees.
- All actual or suspected information security breaches are reported to the Information Security Coordinator and are thoroughly investigated.
- All necessary documentation, including procedures and instructions, exists to support the Policy.
- Aqurance is committed to continually improve the Information Security Management System.
-

The Information Security Coordinator is responsible for maintaining the Policy and providing support and advice during its implementation.

All Managers are directly responsible for implementing the Policy and ensuring employee compliance in their respective departments.

All employees are responsible for reporting information security incidents.

The policy will be reviewed by the Board of Directors at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy and effectiveness.

February 2016