Information Security Policy Statement

The AQAAR properties is committed to maintaining the confidentiality, integrity, and availability of its information assets, and to continually improving its information security management system (ISMS) in accordance with the requirements of ISO 27001:2022 standard.

The ISMS policy of:

1. AQAAR is determined in to delivering high-quality properties that meet the needs of its clients, and to provide excellent customer service throughout the buying, selling, and leasing process.
2. AQAAR's approach to information security management is based on ISO/IEC 27001:2022 standard and globally accepted best practices as a tool to implement a formal system for protecting the confidentiality, integrity and availability of information to ensure:
    a. It is appropriate to the purpose of the organization
    b. Information is only accessed, approved and/or updated by authorized individuals, who have the required approvals
    c. All the confidential information is well protected with all the necessary controls
    d. Information is only changed and/or updated by authorized individuals
    e. Information is regularly backed-up to ensure that it can be recovered in the event of data loss or corruption
    f. Information is always available to all the individuals who have proper and approved authorization to access this information
    g. All individuals who have been granted any form of access to information are fully accountable for the proper use of this information
3. AQAAR is committed to ensure compliance with applicable legal and regulatory requirements related to information security
4. The IS policy is a tool to provide a framework for setting information security objectives
5. The information security policies, procedures, and standards are documented, communicated to and followed by all management and staff personnel.
6. This policy shall be available to all relevant interested parties as appropriate.
7. Management shall be committed to encourage Information Security continual improvements by engaging with all staff and relevant interested parties.

Every staff member, including the Chief Executive, are required to be knowledgeable about the IS Policy, comply with it and is responsible for its implementation. The Board of Directors is fully supportive of this effort.

The responsibility of ensuring that this policy is comprehended, implemented, and sustained by all levels of management in the Company lies with the Head of IT. The suitability of this Policy is reviewed on an ongoing basis during the Management Review Meetings.

CEO

Company stamp