

Information Security Policy - ISO 27001:2022

The Alkath Group is committed to understanding and effectively managing risks related to Information Security to provide greater certainty and confidence for our security holders, employees, customers, suppliers, and the communities in which we operate. Our aim is to find the right balance between information security risk management and business benefit.

It is the policy of the Alkath Group to ensure:

- Information will be protected against unauthorised access.
- Confidentiality of information will be maintained.
- Information will not be disclosed to unauthorised persons through deliberate or careless action.
- Unauthorised access or modification does not compromise information integrity.
- Information is available to authorised users when needed.
- Information security training is completed by all internal users.
- The competency and integrity of 3rd party users is evaluated and monitored.
- All suspected breaches of information security will be reported and investigated.

To provide such a level of risk management and to ensure business continuity, the Alkath Group has implemented an Information Security Management System (ISMS) in line with the International Standard for Information Security, ISO 27001:2022. This standard defines the requirements for an ISMS that is based on internationally recognised best practices, and we have committed to meeting all applicable information security requirements.

Any individual dealing with information at the Alkath Group, no matter what their status (e.g.; employee, contractor, or consultant), must comply with the information security policies, procedures, and related information security documents of the Group.

Alkath Group's ISMS aims to:

- Ensure appropriate information security requirements and controls have been identified and are documented for stakeholders.
- Have information security controls in the framework of information security policies and procedures.
- Reduce the opportunity for mistakes and misunderstandings to occur when dealing with IT assets and electronic information of the Alkath Group.
- Educate staff to allow them to independently make informed decisions with regard to the secure handling of IT assets and electronic information.
- Assist in the identification and investigation of fraudulent electronic-related activities and cooperate with relevant legal agencies.
- Defend IT assets and information that the Alkath Group governs, owns, manages, maintains, or controls, which are both tangible and intangible, and safeguard IT-related records and documents that exist in all forms – paper and electronic.
- Comply with the needs of the Regulatory Authorities (internal or external) and relevant legislation.
- Identify, through appropriate risk assessment, the value of information assets and understand their vulnerabilities and the threats that may expose them to risk.
- Manage the risks to an acceptable level through the design, implementation and maintenance of appropriate security processes and controls.

The Alkath Group will maintain a full certification to ISO 27001:2022 in order that the effective adoption of information security best practices may be validated by an independent third party, a Registered Certification Body. By doing this, we have committed to continually improving our ISMS and have set relevant information security objectives, for which outcomes will be continually monitored.

This policy applies to all systems, people and processes that constitute the organisation's information systems, including directors, employees, consultants, suppliers and other third parties who have access to Alkath Group systems.

A full version of this Policy may be requested by applying to the Information Security Manager - info@alkath.group



07/04/2024

.....
Phil Guy – Managing Director

.....
Date