Information Security Policy

As we aim to be a “value add” long term partner to our customers, **Seaco** is committed to protecting employee and interested parties’ information, as well as related assets, from all threats. Whether in physical or electronic form, information must be handled with care, respect, and in accordance with legal, moral, and contractual obligations. Seaco is also committed to satisfying all applicable information security requirements.

To safeguard against evolving security threats, Seaco integrates security by design, establishes policies, and provides ongoing training to protect the information we handle. Security controls are implemented to mitigate risks, prevent harm, and ensure uninterrupted business operations and service delivery.

Our approach to information security is guided by three fundamental principles:

- Confidentiality – Ensuring that information is accessible only to authorized individuals.
- Integrity – Preventing unauthorized or erroneous modifications to information.
- Availability – Ensuring that information and services remain accessible when needed.

A comprehensive set of policies applies equally to all employees and any interested parties accessing information. Seaco ensures that they have access to these policies and understand the importance of compliance.

Seaco is committed to the continual improvement of our ISMS. Seaco continuously reviews and updates our policies and security measures to adapt to evolving business needs and emerging threats. By maintaining a proactive and structured risk management approach, Seaco reinforces trust and confidence among our stakeholders.

October 2025