Document ref:	POL-SEC-016
Revision:	1.2
Issued Date	28 / 07 / 2023

Information Security Policy Statement

Nuago is committed to understanding and effectively managing risks related to Information Security to provide greater certainty and confidence for our stakeholders, including employees, customers, suppliers and the communities in which we operate. We strive to balance diligent levels of information security risk with the resulting business benefit to both enhance our performance and minimise potential security exposure. We adhere to the legal, regulatory, and other compliance requirements of our business and industry.

Nuago information security policies are designed to ensure:

- Information is protected against unauthorised access;
- Confidentiality of information is maintained;
- Information is not disclosed to unauthorised persons through deliberate or careless actions;
- Integrity of information is maintained through protection from unauthorised modification;
- Availability of information to authorised users when needed;
- Information Security training and awareness for all staff;
- Suspected breaches of information security are promptly identified, reported, and investigated accordingly.

Any individual or organisations partnering with Nuago, regardless of status (e.g. employee, contractor, or consultant), must comply with the information security policies and related procedures.

Aims and Objectives

The aims and objectives of Nuago's information security policies are to:

- Reduce the opportunity for mistakes and misunderstandings when dealing with the IT assets, information and data of Nuago;
- Educate staff, enabling them to independently make informed decisions with regards to secure handling of IT assets and information owned by Nuago, and when to escalate matters to the relevant internal authorities;
- Ensure information security is addressed for all projects, by way of risk assessments and putting appropriate risk treatments and remediations in place;
- Assist in the identification and investigation of fraudulent information security related activities and co-operate with relevant legal and law enforcement agencies where necessary to do so;
- Defend IT assets and information that Nuago governs, owns, manages, maintains or controls which are both tangible and intangible;
- Safeguard information assets that exist in all forms – paper and electronic – in line with the value and sensitivity of those assets to the business;
- Comply with the requirements of the regulatory authorities, internal or external;
- Comply with legislation and industry best practices as they apply to Nuago;

- Provide information security controls that provide a secure environment for the operation of Nuago's business and employees relative to the business context in which it operates.

Responsibilities

Information Security is the responsibility of every member of staff, regardless of their tenure, all contractors and consultants that work with and for Nuago.

All staff have a responsibility to report perceived and actual incidents relating to information security matters to either the Information Security Officer or to their immediate manager.

Management and staff are responsible for embedding information security risk management into all core business activities, functions and processes. Management is responsible for ensuring staff members have received information security awareness training, including information related to Nuago's risk appetite and general approach to addressing risk in decision-making.

Reference Documents:

Document ID	Document Title
POL-NUA-009	Nuago Integrated Management System (IMS)