

INFORMATION SECURITY POLICY

Document Control

Reference: ISMS DOC.3

Issue No: 3.0

Issue Date: 08/11/2019

Page: 1 of 2

Classification: Open

1. Purpose

The purpose of this document is to define the role that EY-Seren's top management takes in the ISMS. This ensures the commitment to information security, the development and propagation of the policy, and the assignment of appropriate information security roles, responsibilities and authorities.

2. Scope

To define EY-Seren's information security policy and to ensure the appropriate information security roles, responsibilities and authorities are assigned.

3. Responsibilities

- The Information Security Team is responsible for setting and approving the information security policy.
- The CEO is responsible for ensuring that roles, responsibilities and authorities are appropriately assigned, maintained and updated as necessary.
- All Employees are responsible for adhering to the requirements of the information security policy and for fulfilling any duties related to assigned roles, responsibilities or authorities.

4. Information Security Policy Statement

It is EY-Seren's policy to maintain an Information Security Management System designed to meet the requirements of the ISO 27001:2013 Standards in pursuit of its primary objectives, purpose and the context of the organization.

EY-Seren provides satisfaction to all customers, stakeholders and interested parties whenever possible, meeting and exceeding expectations. Customer service is an essential part of the process; therefore, the organization provides all employees with training to ensure awareness and understanding of information security.

EY-Seren ensures the details of this policy are known to all internal and external interested parties; where appropriate and determines the need for communication and by what methods. These include but are not limited to customers and suppliers and their requirements as documented in contracts and specifications.

EY-Seren complies with all legislation, regulations, codes of practice and all other requirements applicable to their activities.

EY-Seren provides all resources; inclusive of equipment, trained and competent staff and any other requirements to enable defined information security objectives to be met.

EY-Seren ensures that all employees are made aware of their individual obligations in respect of this information security policy.

EY-Seren maintains a management system that will achieve the company's objectives and seek continual improvement in the effectiveness and performance of the management system based on "risk".

EY-Seren has set information security objectives using the SMART (Specific, Measurable, Achievable, Realistic and Timed) principles. Objectives are planned and documented; inclusive of

INFORMATION SECURITY POLICY

Document Control

Reference: ISMS DOC.3

Issue No: 3.0

Issue Date: 08/11/2019

Page: 2 of 2

Classification: Open

how each is to be achieved and actions required. Subsequently, the objectives are regularly monitored and reviewed.

To ensure the company maintains its awareness for continuous improvement, the Information Security Management System is regularly reviewed at planned intervals by the Information Security Team in formal Management Reviews to ensure it remains appropriate and suitable to the business.

The Management System is subject to both internal and external audits; as appropriate