Information security policy

1. Purpose and Scope

The policy describes the focal points of the organisation regarding the protection and treatment of information, including personal information. The policy applies to all information assets and operation of the organisation irrespective of the format in which the information is stored, such as electronically, on paper, as knowledge preserved by individuals or communications. The policy, moreover, covers all information assets from third parties that Isavia has in its possession and/or which the organisation has asked a third party to manage on its behalf. The policy applies to all employees, the Board of Directors and contractual entities who have access to the organisation´s information.

2. Policy

Isavia encourages the security of information assets through formal procedures that support continuity in operations and minimise operational risk.

3. Objective

The following must guide all the operations of Isavia:

- Maximise information security including information systems owned by or in the possession of the organisation with regards to confidentiality, integrity and availability[1].
- Information assets must be protected from unauthorised access, to prevent inappropriate use, changes, disclosure or destruction of important and sensitive information.
- Physical security must be acceptable, such as access to the premises of Isavia.
- Encourage and maintain active awareness of information security in the minds of employees and the Board, as well as other entities that are given access to information when working for the organisation.
- Follow laws and regulations on information management, information security and general data protection that apply to the organisation.
- Follow the criteria of the safety standard ÍST EN ISO/IEC 27001:2017 as the foundation for organisational and maintenance actions which ensure confidentiality, integrity and availability of information assets.
- Continuously work on improvements and regularly perform risk assessments to see whether there is a need for information security improvement.

4. Other

The Directors are responsible for all information assets that are formed in their operational unit, and for ensuring that their employees follow the rules and instructions applicable to information security.

The policy is to be presented to employees and other entities that are granted access to sensitive information assets when working for the organisation and is to be accessible on the organisation´s intranet and external website.

Approved by the Managing Director on 10.09.2019

[1] Confidentiality: Ensure information is only accessible to those authorised and in need of access. Integrity: Ensure the accuracy and integrity of information and processing methods. Availability: Information is both accessible and useable to those authorised when required.

This is a translation of the original Icelandic version of the policy which is the valid version, signed by the Managing Director.