ISMS Statement

1. Policy Objectives

- To protect the information assets that Nexstor processes, has access to, and to ensure the on-going maintenance of their confidentiality, integrity, and availability.
- To ensure controls are implemented that provide protection for information assets and are proportionate to their value and the threats to which they are exposed
- To ensure we comply with all relevant legal, regulatory, contractual, and other third-party requirements relating to information security,
- To continually improve our Information Security Management System (ISMS) and its ability to withstand threats that could potentially compromise information security.

2. Scope

This policy and its sub-policies apply to all people (including contractors), processes, services, technology, and assets within the Nexstor ISMS scope statement.

3. Statement of Intent

Nexstor believes that despite the presence of threats to the security of such information, all security incidents are preventable. We are committed to achieving policy objectives through:

- Maintenance of an ISMS that is certified as compliant to ISO 27001 by a UKAS-accredited Certification Body.
- Systematic identification of security threats and the application of a risk assessment procedure that will identify and implement appropriate control measures.
- Regular monitoring of security threats and testing / auditing of control measures effectiveness.
- Maintenance of a risk treatment plan that is focused on eliminating or reducing security threats.
- Maintenance and regular testing of a Business Continuity Plan.
- Clear definition of responsibilities for implementing the ISMS.
- Provision of appropriate information, instruction, and training so that all employees are aware of their responsibilities and legal duties, and can support the operation of the ISMS.
- Implementation and maintenance of all ISMS policies and procedures.

Reference: NS-ISMS-STM
Review: Annually
Last Issue: 11/10/2022

The implementation of this policy is fundamental to our success and must be supported by all employees and contractors who have an impact on information security. The appropriateness and effectiveness of this policy, and the means identified within it, for delivering our commitments will be regularly reviewed by our company Directors. Violations of this policy may be subject to our disciplinary policies. This policy is publicly available to interested external parties upon request.

Rob Townsend
Director

Reference: NS-ISMS-STM
Review: Annually
Last Issue: 11/10/2022