Policy Information: Information Security Management Policy	
Company	Leesman, Data Processor.
Scope of policy	Leesman's objective of managing information security is to ensure that its core and supporting business operations continue to operate with minimal disruptions. Leesman shall ensure that all data that are collected or presented by Leesman have absolute integrity. Leesman policy is that all relevant information is managed and stored with their associated confidentiality procedures.
Data category subject of this policy	Any individual whose data is processed by Leesman.
Policy prepared by	CTO
Date approved by CEO	Yes
Policy review date	21st September 2022, by Fanny Mrani.

Leesman

Leesman Information Security Management Policy

OBJECTIVE
This document is a non-confidential, public facing, high level document outlining Leesman's stance on Infosec. It is deliberately high level to retain the confidentiality of Leesman policies. It can be read alongside the Leesman Security Statement.

Leesman's objective of managing information security is to ensure that its core and supporting business operations continue to operate with minimal disruptions. Leesman shall ensure that all data that are collected or presented by Leesman have absolute integrity. Leesman policy is that all relevant information is managed and stored with their associated confidentiality procedures.

STAKEHOLDERS
The CEO has approved the Information Security Policy.

POLICY
The purpose of the Policy is to protect the organisation's information assets[1] from all threats, whether internal or external, deliberate or accidental.

It is the Policy of the organisation to ensure that:

Information should be made available with minimal disruption to staff and the public as required by the business process[2]

The integrity of this information will be maintained [3]

Confidentiality of information not limited to research, third parties, personal and electronic communications data will be assured [4]

Regulatory and legislative requirements will be met [5]

A Business Continuity Policy shall be made available and Business Continuity plans will be produced to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters. Business continuity plans should be maintained and tested[6]

Information security education, awareness and training will be made available to staff [7]

All breaches of information security, actual or suspected, will be reported to, and investigated by the relevant authorities not limited to System Administration and Incident Response [8]

Appropriate access control will be maintained, and information is protected against unauthorised access.

Leesman

Policies, Procedures and Guidelines not limited to Information Security will be made available in the company online information portal to support the ISMS Policy.

Technology Group has direct responsibility for maintaining the ISMS Policy and involved with writing and/or managing the development of relevant policies, procedures and guidelines not limited to information security.

All managers are directly responsible for implementing the ISMS Policy within their units, and for adherence by their staff.

It is the responsibility of each member of staff to adhere to the ISMS Policy.

Information security is managed through Leesman's Risk Management framework.

The availability of information and information systems will be met as required by the core and supporting business operations.

---

[1] Leesman is operationally a cloud-based business.
[2] This will ensure that information and vital services are available to users when and where they need them.
[3] Safeguarding the accuracy and completeness of information by protecting against unauthorised modification.
[4] The protection of valuable or sensitive information from unauthorised disclosure or unavoidable interruptions. Leesman does not store sensitive of confidential data.
[5] Leesman will comply with the relevant business laws and legislations such as: GDPR, Companies Act and the Data Protection Act.
[6] Business Continuity Management should be implemented effectively to ensure continuity of business operations in the event of a crisis or disaster.
[7] Ensure that relevant and effective training is provided to staff.
[8] Ensure that the staff understand their roles and responsibilities in handling incidents and have a comprehensive and well-tested incident response plan ready. The policy will be reviewed by Leesman's ISMS Team annually.

For more information, please contact one of the below:

- Technical Onboarding Specialist

Fanny Mrani, fanny.mrani@leesmanindex.com

- Chief Technology Officer & Data Protection Officer

Allen Green, allen.green@leesmanindex.com