INFORMATION SECURITY POLICY

For Mindspace Business Parks REIT



INFORMATION SECURITY POLICY

Purpose

The Information Security Policy (”Policy”) is applicable to Mindspace REIT, its Special Purpose Vehicles of Mindspace REIT (”SPVs”) (“Mindspace REIT Group”) and Manager. Mindspace Business Parks REIT (“**Mindspace REIT**”) is a part of K Raheja Corp group. Mindspace REIT’s network has adopted the ISO/IEC 27001:2022 Information Security Standard which applies a risk-based approach to protect information assets. The ISO/IEC 27001:2022 Information Security Standard is internationally renowned and provides the best practices for managing information security risks and controls within the framework of an information security and risk management program to support the Policy and business objectives. The purpose of the Information Security Policy is to ensure cybersecurity of systems and respect data privacy towards information security and responsible usage of Artificial Intelligence (AI).

Objectives

The specific objectives of the Information Security Policy are:

- To prevent unauthorized disclosure of information stored or processed on Mindspace REIT’s information systems (Confidentiality)
- To prevent accidental or unauthorized deliberate alteration or deletion of information (Integrity)
- To ensure that information is available to authorized people whenever required (Availability)

To ensure that all AI systems comply with applicable data protection, privacy, information security requirements, and relevant regulatory obligations (Legality)The Policy will provide guidance to ensure that Mindspace Business Parks REIT’s information systems comply with relevant laws and regulations, industry-leading practices and recognized international standards on the information security management system.

Scope

Information Security Management Systems (ISMS) applies to IT Infrastructure and its associated services, namely, IT Delivery, Infrastructure, AI systems and Security Operations along with support functions HR and Admin to provide secure and quality services to its customers.

Policy Framework

The ISMS is committed to continual improvement of Information Security by satisfying applicable requirements relating to Information Security. Information assets are critical to the success of our business. Mindspace Business Parks REIT shall, therefore, ensure the confidentiality, integrity, availability and legality of the information and information processing assets of its customers and the REIT by deploying appropriate people, processes, and technology. Additionally, the ISMS shall integrate clear accountability and distinct labelling of AI outcomes, define boundaries for what AI can and cannot do, and limit accessibility to sensitive AI capabilities (e.g., surveillance etc.) to promote transparency of AI results and avoid potential bias in AI usage.

- All employees of Mindspace REIT’s network and third-party users shall be responsible for adhering to and remain in compliance with the ISMS and ethical usage of deployed AI systems in accordance with the policies and procedures.
- All employees of Mindspace REIT’s network and third-party users shall understand their roles and responsibilities towards implementing ISMS security controls and ensuring human intervention(s) in critical decision-making for AI-driven outcomes.

- The Information Security Policy shall be communicated to all employees through onboarding and periodic training as well as by storing it in some shared location or publishing it on the website of the Organization.
- The Information Security Policy should be communicated to all interested parties.

Policy Statement

Mindspace Business Parks REIT has obtained ISO/IEC 27001:2022 certification for their Information Security Management System (ISMS). The certification, issued by Intertek, covers centralized IT, HR, and administration functions across multiple locations, including the corporate headquarters. This certification underlines the Mindspace REIT's commitment to maintaining robust information security practices and compliance with global standards.

Vulnerability Management Policy

This policy is committed towards the protection of IT infrastructure including servers, applications, network, databases, AI systems and security devices with security, reliability, fairness, avoidance of bias and stability through periodic assessments and internal audits to detect potential vulnerabilities like data breaches, drift or degradation of AI models over time etc. The technical vulnerabilities of Information Systems and infrastructure shall be regularly identified and evaluated to ensure adequate measures are taken to address the associated risks. All discovered vulnerabilities are assigned a Common Vulnerability Scoring System (CVSS) and shall be reported and addressed appropriately to mitigate the identified risks within specified timelines.

Supplier Management

The purpose of this policy is to ensure that Mindspace REIT's suppliers, vendors and third-party contracts follow information security requirements while accessing and managing the REIT's information assets for service delivery and/or during service delivery.

Information Security Incident Management (ISIM)

A security incident is defined as any event which affects confidentiality, integrity or availability of data in the enterprise. Security incidents can be successfully managed by having a clear incident management policy in place.

a. Information Security Incident Management Policies

The purpose of this policy is to define standard methods for identifying, tracking, promptly responding and remediating IT Security Incidents.
ISIM applies to all physical, network and computing assets owned and/or administered in the enterprise. All Employees of the entity are required to follow this procedure for reporting Information Security weaknesses and incidents. Our IS Head / Chief Information Officer (CIO) is responsible for information security implementation and best practices within the organization.

b. Business Continuity Program (BCP)

BCP focuses on continuity of critical business processes. Each document shall be updated on a periodic basis and records of the same shall be maintained. This policy enforces a consistent way to maintain, evaluate and update the Business Continuity Management (BCM) documentation and ensure that changes to the documents are performed in a controlled and systematic manner.
The incident response plan shall be used in the event of system compromise addressing specific incident response procedures, business recovery and continuity procedures, data backup processes, roles and

responsibilities, and communication and contact strategies. The plan is tested periodically, and appropriate training shall be provided for staff with security breach response responsibilities.

All documents are prepared in accordance with ISO 27001:2022.

Compliance

The information systems should be regularly reviewed for compliance with the information security policies and standards & IT Act.

Definitions

Terms	Definition
Asset	Anything tangible or intangible that can be owned controlled and produce value through its use.
Availability	Property of being accessible and usable on demand by an authorized entity.
Backup	The saving of files onto alternate storage or other offline mass storage media for preventing loss of data in the event of equipment failure, destruction, or accidental deletions.
Business Continuity	The Organization's ability to ensure operations and core business functions are not severely impacted by disaster or unplanned incidents that take critical systems offline.
Confidentiality	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
Copyright	Copyright is a legal right that protects the expression of ideas.
Cryptography	The science of secret writing that enables storage and transmission of data in a form that is available only to the intended individuals
Devices	The device includes all servers, network devices and endpoints.
Document	A document is something that is being currently worked upon and is therefore subject to editing and change.
Encryption	The transformation of plain text into unreadable cipher text.
External Network	Any network including the Internet, outsourced suppliers, and business partners.
Information Systems	Knowledge or information that is retained in electronic form (such as emails, documents, etc.) or physically tangible material (such as printed documents, etc.) for industrial control systems or set of applications, services, information technology assets, or other information-handling components.
Information Security Event	The identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that can be security relevant.

Information Security Management System	Is a management system based on a systematic business risk approach to establish, implement, operate, monitor, review, maintain, and improve information security.
Information Security Incident	Single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
Integrity	Property of accuracy and completeness of the information.
Password	A protected word or string of characters which serves as an authentication of a person's identity, or which may be used to grant or deny access to private or shared data.
Review	The activity was undertaken to determine the suitability, adequacy, and effectiveness of the subject matter to achieve established objectives.
Risk	A potential event or action that would harm the organization.
Risk assessment	The overall process of risk identification, risk analysis and risk evaluation.
Suppliers	Any third-party service providers, vendors, contractors, and their sub-contractors are referred to as supplier.
System	Any machine used for computation which includes endpoints, servers, application.
Third-Party	Third parties include suppliers including advisors, consultants, service providers (contractors and their sub-contractors), vendors and other personnel having access to the Organization's information systems.
Virus	A computer virus is a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its code.
Vulnerability	Vulnerability is a weakness with an organization's assets that have the potential to allow a threat to occur with higher frequency, more significant impact, or both.

Violations

All employees are obligated to report violations of this policy (e.g., confidentiality breaches, data breaches, threats to information security, deploying AI to engage in manipulative behavior, unauthorized surveillance, exploitation of vulnerabilities, social scoring etc.) to the IS-Head / Chief Information Officer (or equivalent) immediately. The ISMS Forum must approve any exceptions to this policy in advance.

Enforcement and Escalation

Failure to comply with the Information Security Policy may result in:

- Withdrawal, without notice, of access to information and/or information resources
- Disciplinary action, up to and including termination
- Civil or criminal penalties as provided by law

References

The Information Security Policy and Responsible AI Usage Policy shall refer to the ISO/IEC 27001:2022 Information Security Standard.