VSJ INVESTMENTS PRIVATE LIMITED

IT AND IS POLICY

Version	Updates	Reviewed Date	Approved by
2024	IT & IS Policy	21/05/2024	Board of Directors

This statement of Information Technology and IS Audit Policy was adopted by the Board of Directors of VSJ Investments Private Limited (“VSJ”). The security policies contained in this document have been established to cover information, data and information systems such as software, hardware, firmware, storage and transmission media and computer networks (collectively referred as ‘Information Assets’) used by VSJ.

This security policy shall apply to any person (such as employees, system administrator or in-charge, users, auditors, contractors, consultants, outsourced vendors, third parties and others) who access VSJ’s information or use VSJ’s information systems at office.

Information Security Steering Officer

Company shall appoint Information Security Steering Officer for Governance of the Policy.

Policy Review and Approval

This policy document shall be reviewed at least annually by the Board of Directors. The policy owner will be responsible to make the changes to the policy document. The Information Security Steering Officer of the Company will be responsible to approve the changes.

Policy statement

The policy shall define the security organization structure which VSJ shall adhere to in order to secure its IT assets.

Policy Purpose

The organization structure for Information Security shall be clearly defined, reviewed and updated as necessary. While defining roles and responsibilities within the organization structure, segregation of duties and the principle of least privilege shall be employed, where applicable, so that incompatible roles are not assigned to the same individual.

Policy scope and applicability

This policy is applicable to all the employees of the Company

I. Information Technology Policy (IS Policy)

Policy sections and clauses

The role of the Information Security Steering Officer(ISSO):

i. Review and approve information security policy and overall responsibilities;

ii. Approve significant changes in the exposure of information assets to major threats;

iii. Approve Risk Analysis and Risk Treatment Plan;

v. Approve major initiatives to augment information security;

vi. Review information security incidents and ensure that the resultant preventive action plan is implemented;

vii. To suspend user ID of staff on long leave, training etc.

viii. Ensure continued compliance with business objectives and external requirements.

ix. Keep the Policy up to date with all the policy, procedures, guidelines, baselines and standards properly documented and available to all the concerned people;

x. Facilitate and coordinate various activities pertaining to implementation and monitoring of Information Security policies and procedures;

xi. Ensuring backup is taken regularly on external drives and External drives are kept properly under safe custody. External drive is stored at remote location.

xii. Maintaining records of Purging of data files. Purged backup media is kept under safe custody. Access to Purged data should be restricted.

xiii. Define information security processes;

xiv. Ensure that provisions are in place for the continued protection of information system resources in the organization;

xv. Prepare the annual information security budget, aligned to the business and IT strategy;

xvi. Initiate and carry out Risk assessment as per the Risk assessment plan;

xvii. Decide and put in place the content for information security awareness sessions;

xviii. Maintain the information security awareness within the organization by planning and conducting training sessions in coordination with Human Resource (HR) department;

xix. Review, analyse, resolve and escalate the information security incidents reported in the organization;

xx. .Review Audit reports and monitor the progress of corrective and preventive actions plans;

xxi. Report the compliance or the lack of compliance to the published Information Security Standards & Regulations;

xxii. Take necessary measures to implement and maintain the security of the information systems;

xxiii. Ensure that the VSJ staff is adequately trained to meet the security requirements of the organization

xxiv. Ensure that the responsibilities are defined for and that procedures are in effect to promptly detect, investigate, report and resolve IT security incidents within the organization;

xxv. To initiate appropriate measures to ensure implementation of security measures at the Data Centre and other related information system resources;

II. Information System (IS) Audit Policy:

i. The company shall conduct bi-annual audits by competent independent party to ensure compliance with the information security policies, procedures, standards and guidelines.

ii. Formal procedures shall be developed for planning and reporting audits and audit findings, and ensuring the implementation of a prompt and accurate remedial action.

iii. Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed upon to minimize the risk of disruptions to business processes.

iv. Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.

v. Arrange for independent information security audits / reviews and facilitate resolution of security related issues reported by the systems in the audit.

Exception handling and Policy violations

Any exceptions to the aforementioned policy shall be documented. Non-compliance to the policy will be considered a violation to the Company’s information security policy.