Fast Capital Markets Limited

POLICY ON THIRD PARTY INFORMATION SECURITY MANAGEMENT

Policy created by	Designated Officer
Policy reviewed by	Technology Committee
Policy reviewed on	31.12.2023
Policy Approved by	Board of Directors
Policy approved on	04.01.2024

Version – 1.0

Purpose and Scope

This Third-Party Information Security Management Policy outlines the procedures and guidelines for managing information security risks associated with third-party relationships within our Company. The objective is to ensure the confidentiality, integrity, and availability of information assets shared with or accessed by third parties.

Third-Party Information Security Risk Assessment

Due Diligence

- Perform thorough due diligence before engaging with third parties.
- Assess the information security practices and controls of potential third-party partners.

Risk Categorization

- Categorize third-party relationships based on the level of information security risk they pose.
- Tailor risk assessments to the specific nature of the relationship.

Contractual Obligations

Information Security Clauses

- Include specific information security clauses in contracts with third parties.
- Clearly define security requirements, responsibilities, and compliance expectations.

Compliance Audits

- Reserve the right to conduct periodic audits to verify third-party compliance with information security requirements.
- Establish protocols for notifying third parties about upcoming audits.

Security Controls and Monitoring

Security Controls

- Specify minimum information security controls that third parties must implement to safeguard shared information.
- Examples include encryption standards, access controls, and data protection measures.

Monitoring Mechanisms

- Implement monitoring mechanisms to track third-party compliance with security controls.
- Establish reporting mechanisms for anomalies or security incidents.

Incident Response and Notification

Incident Response Plans

- Ensure that third parties have incident response plans in place to address security incidents promptly.
- Collaborate on aligning incident response processes.

Notification Requirements

- Define notification requirements in the event of a security incident that impacts shared information.
- Establish clear timeframes for reporting incidents.

Confidentiality and Non-Disclosure

- Emphasize the importance of maintaining the confidentiality of shared information.
- Implement non-disclosure agreements as necessary to protect sensitive data.

Data Handling and Retention

- Define data handling and retention policies for shared information.
- Specify data disposal procedures at the conclusion of the third-party relationship.

Training and Awareness

- Provide training to third-party personnel on information security policies and best practices.
- Promote awareness of the importance of information security within the third-party organization.

Continuous Monitoring and Improvement

- Implement continuous monitoring mechanisms to assess the ongoing effectiveness of third-party information security controls.
- Periodically review and update this policy to reflect changes in technology and regulatory requirements.

Change in the Policy will be adopted as and when required by the company and is binding on all the Staff / Employees /and Directors of the Company.

Fast Capital Markets Ltd

Binay Kumar Agarwal
Designated Officer