Aldan Investments Pvt Ltd
701 Heritage Plaza, Opp. Indian Oil Nagar, JP Road
Andheri (W), Mumbai 400053
CIN: U67120MH1995PTC084811

Password Policy

Version 1.0

1. Introduction and Purpose

1.1 Introduction

The IT Department at M/s Aldan Investments Private Limited plays a critical role in supporting our stock brokerage operations. This risk management policy outlines our commitment to identifying, assessing, and mitigating risks associated with IT systems, data, and operations. It establishes a framework for managing IT risks and ensuring the security, availability, and integrity of our technology infrastructure.

1.2 Purpose The purpose of this policy is to:

- Establish a systematic and proactive approach to identifying, assessing, and managing IT risks within the organization.
- Define roles and responsibilities for managing IT risks.
- Ensure compliance with relevant laws, regulations, and industry best practices.
- Promote a culture of risk awareness, mitigation, and continuous improvement within the IT department.

2. Risk Management Framework

2.1 Roles and Responsibilities

2.1.1 IT Department

- The IT department is responsible for identifying, assessing, and managing IT risks.
- They will implement and maintain appropriate controls and security measures to mitigate risks effectively.
- The IT department will collaborate with other departments to ensure alignment with the overall risk management framework.

2.1.2 Risk Management Committee

- A dedicated risk management committee, comprising representatives from relevant departments, will oversee the IT risk management process.
- The committee will review and approve risk management strategies, policies, and initiatives.
- They will ensure effective communication and coordination across the organization.

2.2 Risk Assessment Methodology

2.2.1 Risk Identification

- The IT department will conduct regular risk assessments to identify potential risks to IT systems, infrastructure, and data.
- Risks may include cyber threats, data breaches, system failures, unauthorized access, and regulatory non-compliance.
- Risk identification will involve internal analysis, vulnerability assessments, threat intelligence, and industry benchmarks.

2.2.2 Risk Analysis and Evaluation

- Identified risks will be analyzed and evaluated based on their potential impact and likelihood of occurrence.
- A risk matrix or other appropriate evaluation method will be used to determine the severity and prioritize risks.
- Risks will be assessed considering their financial, operational, legal, and reputational impacts.

2.3 Risk Mitigation and Controls

2.3.1 Risk Treatment

- The IT department will develop and implement risk treatment plans to mitigate identified risks.
- Treatment options may include risk avoidance, risk transfer, risk reduction, or risk acceptance.
- Controls and safeguards will be implemented to minimize vulnerabilities and mitigate potential impacts.

2.3.2 Security Controls

- The IT department will establish and maintain a robust set of security controls to protect IT systems, networks, and data.
- Controls may include firewalls, intrusion detection systems, antivirus software, access controls, encryption, and regular system patching.
- Security controls will be regularly reviewed, updated, and tested to ensure their effectiveness.

3. Incident Response and Business Continuity

3.1 Incident Response

- The IT department will develop an incident response plan to address and manage IT security incidents and breaches promptly.
- The plan will include defined roles and responsibilities, escalation procedures, communication protocols, and post-incident analysis.

3.2 Business Continuity and Disaster Recovery

- The IT department will establish and maintain business continuity and disaster recovery plans to ensure the availability and resilience of IT systems and services.
- These plans will include backup procedures, recovery strategies, alternate site arrangements, and periodic testing and drills.

4. Training and Awareness

The IT department will provide regular training and awareness programs to employees regarding IT risks, security best practices,