RAIYYAN EXCHANGE

Policy and Procedures

Version 1.2 (Current)

ABN: 14 620 775 313
ACN: 620 775 313
rayex.com.au

1. Risk Management Policy

Objective

Raiyyan Exchange is committed to identifying, assessing, and managing risks related to its business operations. The goal is to maintain risks at acceptable levels while ensuring smooth operations.

Scope

This policy applies to all employees, contractors, and stakeholders involved in Raiyyan Exchange's activities.

Key Principles

- Identify and analyse risks affecting the company.
- Evaluate risks and take appropriate actions.
- Implement control measures to mitigate risks.
- Document risk management processes.
- Monitor and review risks regularly.

Responsibilities

- **Compliance Officer**: Oversees risk management, fraud monitoring, and staff training.
- **Technology Team**: Ensures security and improvements in risk policies.
- **Staff & Contractors**: Must follow risk management policies.

---

2. Access Control Policy

Objective

To ensure that only authorised personnel have access to Raiyyan Exchange's systems and data.

Key Policies

- Access is granted based on job roles and responsibilities.
- All systems require password protection.
- Two-factor authentication is mandatory for sensitive systems.
- Access logs are monitored for security purposes.

Responsibilities

- Employees must keep login credentials secure.
- Administrators grant and revoke access as needed.
- Unauthorised access attempts are reported and investigated.

---

3. Dispute Resolution Policy

Submitting a Dispute

Customers can file a dispute via email at **clp@rayex.com.au** with the following details:

- Transaction ID
- Date and amount
- Reason for dispute
- Any supporting documents

Acknowledgment and Processing

- Disputes are acknowledged within **24 hours**.
- If the dispute involves an **upstream banking partner**, we will escalate it and resolve it as soon as we receive a response.
- Other disputes will be resolved within **7 days**.

Communication

- Customers will receive updates via email throughout the resolution process.

Final Decision

- Once resolved, the customer will be informed of the outcome.
- If a refund is applicable, it will be processed accordingly.

---

4. Information Security Policy

Objective

To protect Raiyyan Exchange's systems and customer data from unauthorised access and breaches.

Key Security Measures

- Data encryption (AES-256) for secure storage.

- Secure network infrastructure to prevent cyber threats.
- Regular security audits and system updates.

Employee Responsibilities

- Employees must follow all security protocols.
- Any suspicious activity must be reported immediately.

---

5. Fraud Management Policy

Objective

To prevent, detect, and respond to fraudulent activities.

Key Policies

- All transactions are monitored for suspicious activities.
- Fraud detection tools and alerts are in place.
- Employees receive training on identifying fraudulent activities.

Reporting Fraud

- Any suspected fraud must be reported to the Compliance Officer.
- Investigations will be conducted, and necessary actions will be taken.

---

6. Change Management & Incident Response

Objective

To ensure that changes to systems and operations are well-managed and that incidents are responded to effectively.

Change Management

- All changes require approval before implementation.
- Changes are tested in a controlled environment before going live.
- Employees are notified about system updates.

Incident Response

- In case of system failure or security breach, the IT team will act immediately.

- Impacted systems will be restored as quickly as possible.
- Users will be informed of any major incidents.

---

7. Privacy Policy

Objective

To protect the personal information of customers and employees.

What We Collect

- Name, contact details, and business information.
- Transaction data and account details.

How We Use Data

- To provide services and process transactions.
- To improve customer experience and security.
- To comply with legal and regulatory requirements.

Data Security

- We use encryption and secure servers to protect data.
- Only authorised personnel have access to sensitive information.

Access & Updates

- Customers can request to update or delete their information.
- Data retention is based on legal and regulatory requirements.

For any inquiries, please contact:
Email: clp@rayex.com.au