LionFinTech AI & Data Privacy Policy

1. Purpose

1.1 LionFinTech Pte. Ltd. (“LionFinTech”, “we”, “our”) is committed to complying with Singapore’s Personal Data Protection Act 2012 (“PDPA”).
1.2 This policy establishes how we collect, use, disclose, and safeguard personal data of our customers, employees, and partners.
1.3 We adopt a strict AI Usage & Data Privacy Framework to ensure sensitive information is never inadvertently shared with external AI tools, cloud services, or unauthorised parties.

2. Scope

2.1 This Policy applies to:

- All employees, contractors, and interns of LionFinTech.
- All forms of personal data handled by LionFinTech, whether in electronic or hardcopy form.
- All interactions with external AI systems (e.g., ChatGPT, GitHub Copilot, third-party SaaS LLMs).

3. Categories of Sensitive Data (Prohibited for External Disclosure)

3.1 Personal Identifiers (Protected under PDPA)

- **Clause 3.1.1: NRIC**
  Employees must not disclose NRIC numbers as NRIC numbers can be used for identity theft, fraud, and unauthorised access to personal services.
- **Clause 3.1.2: FIN**
  Employees must not disclose Foreign Identification Numbers (FIN) as FINs can lead to identity-related fraud for foreign staff or clients.
- **Clause 3.1.3: PASSPORT**
  Employees must not disclose passport numbers as Passport numbers can be misused for identity theft or illegal travel documentation.
- **Clause 3.1.4: CONTACT INFORMATION (mobile numbers, email addresses, home addresses)**
  Employees must not disclose contact information (mobile numbers, email addresses, home addresses) as exposure can result in phishing attacks, spam, harassment, or

social engineering.

- **Clause 3.1.5: SSN**
  Employees must not disclose Social Security Numbers (SSN) as SSNs are sensitive and can lead to identity theft or financial fraud.

- **Clause 3.1.6: PERSON**
  Employees must not disclose their names as personal identifiers may reveal private information about individuals and expose them to identity theft.

3.2 Financial Data

- **Clause 3.2.1: BANK ACCOUNT NUMBER**
  Employees must not disclose bank account numbers as it can lead to unauthorised transactions or account takeover.

- **Clause 3.2.2: CREDIT CARD**
  Employees must not disclose credit card details as exposed credit card information can be directly used for fraud.

- **Clause 3.2.3: TRANSACTION HISTORY**
  Employees must not disclose transaction histories as it reveals private spending behavior, potentially enabling social engineering attacks.

- **Clause 3.2.4: SALARY**
  Employees must not disclose salary, bonuses, or compensation details as exposure risks privacy violations, internal disputes, and reputational damage.

- **Clause 3.2.5: COMMISSION RATE**
  Employees must not disclose commission rates as it reveals internal pay structures and creates confidentiality risks.

- **Clause 3.2.6: AMOUNT OF MONEY**
  Employees must not disclose the amount of money in transactions as exposure can lead to fraud or unauthorised financial decisions.

- **Clause 3.2.7: ACCOUNT BALANCE**
  Employees must not disclose account balances as it may allow account takeover or targeted financial attacks.

- **Clause 3.2.8: BUDGET**
  Employees must not disclose internal budget details as it reveals company planning and resource allocation.

- **Clause 3.2.9: INVOICE ID**
  Employees must not disclose invoice IDs as it could allow fraudulent invoicing or tampering.

- **Clause 3.2.10: PO NUMBER**
  Employees must not disclose purchase order numbers as it can be misused for unauthorised transactions.

- **Clause 3.2.11: FINANCIAL REPORT**
  Employees must not disclose internal financial reports as exposure may reveal confidential company financial health.

- **Clause 3.2.12: PRICING TERM**
  Employees must not disclose pricing terms as it can give competitors an unfair advantage or affect client relationships.

3.3 Authentication & Access Credentials

- **Clause 3.3.1: API KEY**
  Employees must not disclose API keys as API keys can grant unauthorised access to company or third-party systems.

- **Clause 3.3.2: ACCESS TOKEN**
  Employees must not disclose access tokens as it may allow attackers to impersonate employees and extract sensitive data.

- **Clause 3.3.3: PASSWORD**
  Employees must not disclose passwords as it can compromise both personal and corporate accounts.

- **Clause 3.3.4: ENCRYPTION KEY**
  Employees must not disclose encryption keys as exposure can decrypt confidential files or communications.

- **Clause 3.3.5: SOURCE CODE WITH CREDENTIALS**
  Employees must not disclose source code containing embedded credentials as it could result in intellectual property theft and compromise internal systems.

3.4 Business Confidential Information

- **Clause 3.4.1: PROJECT CODE**
  Employees must not disclose internal project codenames (e.g., “Project LionX”) as

disclosure may reveal ongoing initiatives and competitive advantage.

- **Clause 3.4.2: PRODUCT ROADMAP**
  Employees must not disclose product roadmaps and unreleased features as exposure can harm market positioning or allow competitors to copy plans.

- **Clause 3.4.3: STRATEGIC BUSINESS PLANS**
  Employees must not disclose strategic business or financial plans as it reveals market strategy, potential M&A activities, or revenue plans.

- **Clause 3.4.4: VENDOR AND PARTNER CONTRACTS**
  Employees must not disclose vendor and partner contracts as it breaches confidentiality agreements and damages business relationships.

4. Employee Responsibilities

- **Clause 4.1:** Employees must never input or transmit sensitive data into external AI tools as external AI tools are outside LionFinTech's control and may expose data.

- **Clause 4.2:** Obfuscation of sensitive data does not provide protection as AI systems can infer or reconstruct disguised identifiers.

- **Clause 4.3:** Sensitive data must remain within authorised LionFinTech systems as this ensures compliance with PDPA and MAS TRM security standards.

- **Clause 4.4:** Accidental disclosure of sensitive data must be reported immediately to the DPO as prompt reporting allows mitigation and demonstrates compliance.

5. PDPA Compliance Clauses

- **Clause 5.1:** Personal data must not be disclosed without individual consent (Section 13).

- **Clause 5.2:** Data must only be used for intended, lawful purposes (Section 18).

- **Clause 5.3:** Organisations must protect personal data from unauthorised access, use, or disclosure (Section 24).

- **Clause 5.4:** Personal data must be deleted when it no longer serves a legal or business purpose (Section 25).

6. Monitoring & AI Compliance Firewall

- **Clause 6.1:** All AI interactions within LionFinTech are monitored in real-time.
- **Clause 6.2:** Prompts sent to external AI systems are automatically scanned by LionFinTech's Policy-Aware AI Privacy Guardian.
- **Clause 6.3:** The system flags, blocks, or masks sensitive data and logs violations per policy clauses.

7. Data Protection Officer (DPO)

- **Clause 7.1:** LionFinTech has appointed a DPO to oversee PDPA compliance.
  Contact: [Insert DPO Name & Email]

8. Enforcement & Consequences

- **Clause 8.1:** Non-compliance may result in mandatory retraining on PDPA and internal data privacy.
- **Clause 8.2:** Repeated or serious breaches may lead to disciplinary action, including termination.
- **Clause 8.3:** Breaches may be reported to the Personal Data Protection Commission (PDPC).

9. Review & Updates

- **Clause 9.1:** This policy will be reviewed annually or whenever PDPA or MAS guidelines are updated.