SuprFi Information Security Policy

Effective Date: November 10, 2025
Approved by: Doug Rose, Chief Operating Officer

---

1. Purpose

The purpose of this Information Security Policy is to establish and maintain a framework that safeguards SuprFi's information assets, systems, and data from unauthorized access, disclosure, alteration, and destruction. This policy ensures that SuprFi identifies, mitigates, and continuously monitors information security risks relevant to our business operations, technology platforms, and customer data.

---

2. Scope

This policy applies to all employees, contractors, vendors, and systems that process, store, or transmit company or customer data.
It covers all SuprFi facilities, hardware, software, cloud services, and third-party integrations including Plaid, financial institutions, and CRM partners.

---

3. Governance and Accountability

- The **COO (Doug Rose)** serves as the executive sponsor for information security.
- The **Security & Compliance Lead** (designated internally) is responsible for policy maintenance, risk assessments, and incident coordination.
- All staff must comply with this policy and complete annual security training.
- Policy violations may result in disciplinary action or termination of access.

---

4. Risk Management

SuprFi maintains a continuous risk management program designed to identify, evaluate, and mitigate security risks.

- **Risk Assessments** are conducted annually and upon significant changes to infrastructure or data flows.
- Risks are prioritized by likelihood and impact and tracked through a remediation log.
- Critical risks must be mitigated within 30 days or escalated to executive leadership.

---

5. Data Classification & Handling

All information assets are classified into the following categories:

1. **Public:** Approved for open disclosure.
2. **Internal:** Restricted to SuprFi personnel.
3. **Confidential:** Sensitive business information.
4. **Restricted:** Personally identifiable information (PII), financial data, and partner credentials.

Handling requirements:

- Restricted data must be encrypted in transit (TLS 1.2+) and at rest (AES-256).
- No customer financial data is stored locally or shared via unsecured channels.
- Logs containing PII are masked or tokenized before use in analytics.

---

6. Access Control & Authentication

- Access to systems follows the **principle of least privilege**.
- Role-based access control (RBAC) is enforced for all production systems.
- MFA (Multi-Factor Authentication) is required for administrative access.

- Access rights are reviewed quarterly and upon termination or role change.
- Shared credentials are prohibited.

---

7. Encryption & Key Management

- All sensitive data is encrypted using **AES-256** for storage and **TLS 1.2+** for transmission.
- Encryption keys are managed securely via AWS KMS and rotated annually or upon personnel changes.
- Secrets and API keys are stored using secure vaulting services (e.g., AWS Secrets Manager).
- No hard-coded credentials are permitted in application code.

---

8. Network & Infrastructure Security

- Cloud environments (AWS) are configured following CIS benchmarks.
- Firewalls and network access controls are used to restrict traffic to necessary ports and protocols.
- Security patches and updates are applied monthly, or within 72 hours for critical vulnerabilities.
- Continuous monitoring and alerting are implemented using logging and threat detection tools.

---

9. Vendor and Third-Party Security

SuprFi evaluates all vendors handling sensitive data before engagement.

- Vendors must adhere to comparable security and privacy standards.

- Security reviews are conducted annually.
- Third-party connections (e.g., Plaid, KYC, CRMs) use encrypted APIs with access keys and audit trails.
- Contracts include confidentiality and data protection clauses.

---

10. Physical Security

Although SuprFi operates primarily remotely, any physical office or data storage location must:

- Use controlled access (e.g., badges, locks, or keypads).
- Restrict visitor access and maintain sign-in logs.
- Prohibit leaving printed or unsecured documents in public areas.
- Require devices to be stored securely when unattended.

---

11. Incident Response & Breach Notification

SuprFi maintains an **Incident Response Plan** (IRP) defining procedures for detecting, containing, investigating, and resolving security incidents.

- All employees must report suspected incidents immediately to the Security Lead.
- Incidents are logged and reviewed within 24 hours.
- Affected parties and regulators are notified per applicable laws and contractual obligations.
- Post-incident reviews identify root causes and preventive actions.

---

12. Business Continuity & Disaster Recovery

- SuprFi maintains a **Business Continuity Plan (BCP)** and **Disaster Recovery Plan (DRP)** to ensure minimal downtime.
- All critical systems are hosted on redundant, geographically diverse cloud infrastructure.
- Daily backups are encrypted and stored in separate AWS regions.
- DR drills are conducted at least annually.

---

13. Security Awareness & Training

- New hires receive onboarding on data handling, phishing prevention, and incident reporting.
- Annual refresher training is mandatory for all staff.
- Simulated phishing and awareness campaigns are conducted quarterly.

---

14. Policy Maintenance and Review

- This policy is reviewed annually or when material changes occur to business operations or infrastructure.
- Updates are approved by the COO and communicated company-wide.
- The latest version is stored in the company's compliance documentation repository.

---

15. Acknowledgment

All employees, contractors, and vendors with system access must acknowledge they have read, understood, and agree to comply with this policy.

---

16. Approval and Signature

Approved By:
Doug Rose
Chief Operating Officer, SuprFi

Signature: 
Date: *11/11/2025*