

Focus Notebook Information Security Policy

Focus Notebook

November 12, 2025

1 Purpose & Scope

This policy defines how Focus Notebook protects the confidentiality, integrity, and availability of customer data processed through our Firebase-backed platform. The policy covers all employees, contractors, systems, and vendors that interact with production or customer data, including Google Cloud Platform (GCP), Firebase services, Stripe, Plaid, and AI providers.

2 Governance

- The Chief Technology Officer (CTO) owns this policy, reviews it at least annually, and reports material risks to company leadership.
- All personnel must acknowledge the policy during onboarding and whenever substantive updates are made.
- Security requirements are embedded in our SDLC through peer review, automated checks, and deployment gates.
- Risks are tracked in the internal issue tracker with owners, mitigation dates, and validation notes.

3 Risk Management

- Conduct a lightweight risk assessment twice per year focused on Firebase, Plaid, Stripe, and data pipeline changes.
- Prioritize risks based on impact and likelihood; document resulting controls or compensating measures.
- Require architectural review before onboarding new data processors or deploying new Firebase regions.

4 Access Control

- Use Google Workspace identities with enforced MFA for all engineering accounts.
- Apply least-privilege IAM roles in GCP/Firebase; production deploy access is limited to the on-call engineering team.

- Service accounts are scoped per environment; secrets such as Plaid tokens are injected via Firebase Secret Manager and never committed to source control.
- Access reviews occur quarterly; stale accounts or unused roles are removed within five business days.

5 Data Protection

- Data is classified as Public, Internal, Sensitive, or Highly Sensitive. Plaid-derived banking data and PII are Highly Sensitive.
- All data in Firebase (Firestore, Storage) inherits Google-managed encryption at rest; TLS 1.2+ is enforced for data in transit.
- Sensitive exports (e.g., CSV statements) are deleted once processed unless a product requirement mandates retention; retention schedules are documented per dataset.
- Encryption keys are managed by GCP KMS; overrides require CTO approval and change management.

6 Application & Infrastructure Security

- Firestore and Storage security rules enforce per-user access, verified via automated tests before deployment.
- Cloud Functions use the minimum necessary permissions; environment configuration is stored in Firebase Secrets and Config.
- Dependencies are scanned via GitHub Dependabot and npm audit; critical advisories are patched within seven days.
- All production changes require pull-request review and automated CI (lint, tests, build) before deployment.

7 Monitoring & Logging

- Cloud Logging captures application logs, admin actions, and IAM events; logs are retained for at least 90 days.
- Alerts notify the on-call engineer of elevated error rates, failed deployments, and suspicious authentication events.
- Weekly log reviews confirm no unauthorized access occurred; findings feed into the risk register.

8 Incident Response

- Incidents follow four stages: Detect, Triage, Contain/Eradicate, and Recovery/Postmortem.
- Severity definitions determine notification timelines; Plaid and affected customers are notified within 24 hours of confirming exposure of financial data.
- Postmortems are completed within five business days and include remediation owners and due dates.

9 Business Continuity & Backup

- Firestore managed backups or scheduled exports run daily; restore procedures are tested quarterly in a staging project.
- Infrastructure-as-code (firebase.json, rules, deployment scripts) is version-controlled to enable rapid rebuilds.
- Critical vendor outages (GCP, Plaid, Stripe) are tracked via status feeds; runbooks document fallback steps.

10 Vendor & Third-Party Management

- Maintain an inventory of critical vendors with contract owner, data processed, and compliance posture (SOC 2/ISO 27001).
- Require DPAs and security documentation before onboarding vendors handling Sensitive or Highly Sensitive data.
- Review vendor security attestations annually; high-risk vendors undergo penetration testing or independent audits when available.

11 Physical Security & Device Management

- Production systems run exclusively on Google data centers; we rely on Google's physical controls (SOC 2 Type II).
- Employee devices use full-disk encryption, screen auto-lock (>5 minutes), and company-managed endpoint protection.
- Lost or stolen devices are reported within one hour and remotely wiped; replacements require fresh security posture verification.

12 Training & Awareness

- Security awareness training is required at hire and refreshed annually, covering phishing, data handling, and incident reporting.
- Engineers receive role-specific training on Firebase security rules, secret management, and compliance obligations.

13 Policy Maintenance

- This policy is reviewed annually or upon major platform changes; revisions are versioned and communicated to all staff.
- Exceptions require written approval from the CTO, include an expiration date, and are tracked in the risk register.