Non-Functional Requirements (NFR): Drop — Fintech Payment App

Non-Functional Requirements (NFR): Drop — Fintech Payment App

> **Project:** Drop — Remittance + QR Payments **Version:** 1.0 **Date:** 2026-02-23
> **Author:** John (AI Director) **Status:** Approved **Reviewers:** Alem Bašić (CEO)

Document History

Version	Date	Author	Changes
0.1	2026-02-23	John	Initial draft; targets from security audit + business case

---

1. NFR Overview

Category	# Requirements	Highest Priority	Owner
Performance	6	Must Have	John (Tech Lead)
Scalability	4	Must Have	John / DevOps
Availability	6	Must Have	John / DevOps
Security	12	Critical	John + Security agent

Category	# Requirements	Highest Priority	Owner
Reliability	5	Must Have	John
Usability	5	Should Have	John (Designer)
Compatibility	4	Must Have	John
Maintainability	5	Should Have	John
Compliance	8	Critical	John + Legal
Data	5	Must Have	John

2. Performance Requirements

ID	Requirement	Metric	Target	Measurement Conditions	Method	Priority
NFR-P01	Page load time (initial)	Time to Interactive	< 3 seconds	4G connection, cold cache	Lighthouse	Must Have
NFR-P02	API response time (standard)	p95 response time	< 500ms	Normal load (200 concurrent users)	APM / k6	Must Have
NFR-P03	API response time (bcrypt operations)	p95 response time	< 1,000ms	Normal load	Benchmark tests	Must Have
NFR-P04	Database query time	p95 query time	< 10ms (SELECT), < 20ms (INSERT)	Normal load	api-benchmarks.test.ts	Must Have
NFR-P05	Core Web Vitals: LCP	Largest Contentful Paint	< 2.5 seconds	Mobile, 4G	Lighthouse	Must Have
NFR-P06	50 concurrent rate limit checks	Total time	< 2,000ms total	50 concurrent calls	api-benchmarks.test.ts	Should Have

3. Scalability Requirements

ID	Requirement	Metric	MVP Target	Phase 2 Target	Method	Priority

NFR-S01	Concurrent users	Active sessions	200 users (SQLite limit)	5,000+ users (PostgreSQL)	Load testing	Must Have
NFR-S02	Database migration trigger	Concurrent users	Migrate at 200 concurrent	PostgreSQL in Phase 2	Monitoring	Must Have
NFR-S03	API rate limits	Max requests per IP	10 req/min (auth), 60 req/min (general)	Same	Rate limiter config	Must Have
NFR-S04	Storage growth	DB size	< 1GB on Fly.io persistent volume	Managed PostgreSQL	Storage monitoring	Should Have

4. Availability Requirements

ID	Requirement	Target	Period	Exclusions	Priority
NFR-A01	System uptime SLA	≥ 99.5%	Monthly rolling	Scheduled maintenance (advance notice)	Must Have
NFR-A02	Scheduled maintenance window	Max 4 hours/month	Monthly	Tue-Thu 02:00-06:00 CET preferred	Must Have
NFR-A03	Maintenance notice lead time	≥ 24 hours	Per event	Emergency patches: ASAP notify	Must Have
NFR-A04	RPO (Recovery Point Objective)	Max 24 hours data loss	Per incident	Daily backup schedule	Must Have
NFR-A05	RTO (Recovery Time Objective)	System restored within 4 hours	Per incident	For staging; production target 2 hours	Must Have
NFR-A06	Database backup	Daily automated backup	Ongoing	Fly.io persistent volume	Must Have

SLA Reference:

Uptime %	Monthly Downtime
99.9%	43.8 minutes
99.5%	3.6 hours
99.0%	7.3 hours

5. Security Requirements

Context: Drop is a fintech app handling real money flows. Security is Critical priority. See `security/drop-security-rapport.md` for full audit (score: 57/100 pre-Phase 0.5; target: 80/100 post-hardening).

ID	Requirement	Category	Target / Standard	Method	Priority
NFR-SEC01	Authentication	Auth	JWT (jose library) in httpOnly cookie; SameSite=Strict; 7-day expiry	Code review + audit	Must Have
NFR-SEC02	Password hashing	Auth	bcrypt, 12 rounds; NO SHA-256 fallback	auth.test.ts	Must Have
NFR-SEC03	JWT secret	Secrets	JWT_SECRET must be set via env var — fail fast if missing	Code review	Must Have
NFR-SEC04	CSRF protection	Injection	CSRF middleware on all POST/PATCH/DELETE endpoints	Code review + test	Must Have
NFR-SEC05	Rate limiting	Abuse	10 req/min on auth; 60/min general; persistent (DB-backed, not in-memory)	middleware.test.ts	Must Have
NFR-SEC06	Input validation	Injection	All inputs sanitized server-side; parameterized SQL (no raw queries)	validation.test.ts	Must Have
NFR-SEC07	XSS prevention	Injection	CSP headers (script-src 'self'); no dangerouslySetInnerHTML	OWASP ZAP	Must Have
NFR-SEC08	Security headers	HTTP	HSTS, X-Frame-Options: DENY, X-Content-Type-Options: nosniff, CSP	securityheaders.com	Must Have

ID	Requirement	Category	Target / Standard	Method	Priority
NFR-SEC09	Card data	PCI-DSS	NEVER store or return full card number or CVV; only last_four + token_ref	Code review + db.test.ts	Must Have
NFR-SEC10	Audit logging	Compliance	All auth events, transactions, KYC changes logged with user_id + IP + timestamp	Code review	Must Have
NFR-SEC11	Per-user transaction locks	Financial	Concurrent transactions from same user serialised; no double-spend	Integration test	Must Have
NFR-SEC12	Penetration testing	Operations	External pentest before production launch	Third-party report	Should Have

6. Reliability Requirements

ID	Requirement	Metric	Target	Method	Priority
NFR-R01	Application error rate	5xx errors / total requests	< 0.1%	Monitoring	Must Have
NFR-R02	Transaction integrity	Atomic transactions	ACID compliance; no partial updates	db.test.ts	Must Have
NFR-R03	MTTR	Average recovery time	< 4 hours	Incident log	Must Have
NFR-R04	Data integrity	Database constraints	Zero orphaned records; FK constraints enabled	db.test.ts	Must Have
NFR-R05	Health check	System observability	GET /api/health returns 200 with DB status	CI smoke tests	Must Have

7. Usability Requirements

ID	Requirement	Target	Method	Priority
NFR-U01	Onboarding completion	New user completes onboarding (3 steps) in < 3 minutes	Usability testing	Must Have
NFR-U02	Remittance flow time	Registered user sends money in < 2 minutes	Usability testing	Must Have
NFR-U03	Mobile responsiveness	Fully functional on 375px–1440px (primary: 375-428px mobile)	Manual + automated	Must Have
NFR-U04	Error recovery	User can recover from any form error without page reload	Manual testing	Must Have
NFR-U05	Language	Norwegian (primary) and English (secondary)	Content audit	Should Have

8. Compatibility Requirements

ID	Requirement	Category	Target	Priority
NFR-C01	Web browsers	Browser	Chrome 100+, Firefox 100+, Safari 16+, Edge 100+	Must Have
NFR-C02	Mobile browsers	Browser	Safari iOS 15+, Chrome Android 100+ (primary platform)	Must Have
NFR-C03	Screen resolutions	Responsive	375px (iPhone SE) to 1440px (desktop); mobile-first	Must Have
NFR-C04	API versioning	API	Next.js API Routes (no versioning in MVP); semantic versioning in Phase 2	Should Have

9. Maintainability Requirements

ID	Requirement	Metric	Target	Method	Priority

NFR-M01	Test coverage	% code covered	≥ 80% overall; 100% for auth + transaction paths	CI coverage (Vitest)	Must Have
NFR-M02	CI/CD pipeline	Deployment frequency	Bug fix to staging in < 30 minutes from merge	GitHub Actions	Must Have
NFR-M03	Feature flags	Feature control	All gated features controllable via env vars without redeploy	feature-flags.test.ts	Should Have
NFR-M04	Documentation currency	Doc coverage	All API endpoints documented in docs/backend/API-REFERENCE.md	Doc review	Should Have
NFR-M05	Dependency currency	CVE exposure	0 critical CVEs in production dependencies	npm audit in CI	Must Have

10. Compliance Requirements

ID	Regulation	Applicability	Requirement	Technical Implementation	Priority
NFR-COMP01	GDPR (EU)	Yes — Norwegian users	Lawful basis; right to deletion; DPA with BaaS; 72h breach notification	Data deletion API; audit logs; DPA contract	Must Have
NFR-COMP02	GDPR — Data minimisation	Yes	Collect only data necessary for stated purpose	BA review of DB schema	Must Have
NFR-COMP03	PSD2 (EU)	Yes — payment initiation	PISP/AISP registration with Finanstilsynet; or operate under bank partner licence	Finanstilsynet registration	Must Have
NFR-COMP04	AML / AMLD6	Yes — money transfer	KYC verification before transaction; transaction monitoring; SAR capability	Sumsub integration; monitoring alerts	Must Have

ID	Regulation	Applicability	Requirement	Technical Implementation	Priority
NFR-COMP05	PCI-DSS	Partial (cards feature)	No card number/CVV storage; tokenisation only	last_four + token_ref only; tokenisation via partner	Must Have
NFR-COMP06	DORA (EU)	Yes	ICT risk management; incident reporting framework	Incident report template; business continuity	Should Have
NFR-COMP07	Norwegian Personvernloven	Yes	National GDPR implementation; same requirements	Legal review	Must Have
NFR-COMP08	Financial licence disclaimer	Yes	NEVER use "banking" without licence disclaimer in UI	UI copy review; `/learning-opportunity` on violations	Must Have

11. Data Requirements

ID	Requirement	Category	Target	Implementation	Priority
NFR-D01	Data retention — user data	Retention	User data deleted within 30 days of account deletion request	Scheduled deletion job (GDPR Art.17)	Must Have
NFR-D02	Data retention — audit logs	Retention	Audit logs: 5 years (AML requirement)	Log rotation policy	Must Have
NFR-D03	PII field documentation	Privacy	All PII fields identified in DATABASE-SCHEMA.md	Data dictionary in docs/backend/	Must Have
NFR-D04	Data anonymisation (non-prod)	Privacy	No real user data in staging/dev environments	Seed data only; no prod data migration	Must Have
NFR-D05	GDPR data export	Portability	User can export their data (GDPR Art.20)	Data export endpoint	Should Have

12. NFR Testing & Verification Plan

NFR Category	Testing Method	Tools	Frequency	Pass Criteria
Performance	Benchmark tests + load testing	api-benchmarks.test.ts, Lighthouse	Per sprint + pre-launch	All NFR-P targets met
Security	Security audit + automated tests	validation.test.ts, OWASP ZAP, external pentest	Per sprint + pre-launch	Score ≥ 80/100; no critical open
Availability	Uptime monitoring	Fly.io metrics, health endpoint	Ongoing	≥ 99.5% monthly
Compliance	Legal review + audit	Manual + Sumsub	Pre-launch + annual	All compliance items verified
Reliability	Unit + integration tests	Vitest (db.test.ts)	Per commit	Zero failed integrity tests

Approval

Role	Name	Date	Signature
Author	John (AI Director)	2026-02-23	Approved (AI)
Tech Lead	John	2026-02-23	Approved
AI Director (John)	John	2026-02-23	Approved
CEO (Alem)	Alem Bašić	TBD	

Revision #6
Created 2026-02-23 12:04:26 UTC by John
Updated 2026-05-31 20:03:05 UTC by John