Index  
[Section 0 – Vision & Policy Baseline](#Section0)  
[Section 1 – Product Vision, Personas, & Journeys](#Section1)  
[Section 2 – Platform Economics, Pricing, & Policy](#Section2)  
[Section 3 – Role Assignment & Onboarding](#Section3)  
[Section 4 – Performance, Accessibility, & UX Standards](#Section4)  
[Section 5 – Risk, Fraud, & Abuse](#Section5)  
[Section 6 – Privacy, Data Retention, & Legal](#Section6)  
[Section 7 – External API’s & Webhooks](#Section7)  
[Section 8 – Database Schema](#Section8)  
[Section 9 – Marketing CMS & Public Pages](#Section9)  
[Section 9B – CMS & Marketing](#Section9)  
[Section 10 – User Portal](#Section10a)  
[Section 11 – Identity & Verification](#Section11)   
[Section 12 – Campaign Creation & Rewards](#Section12)  
[Section 13 – Campaign Public Page](#Section13a)  
[Section 13B – Campaign Public Page](#Section13b)  
[Section 14 – Donation & Checkout Flow](#Section14)  
[Section 15 – Payouts & Cashout](#Section15)  
[Section 16 – Public Website & Discovery](#Section16)  
[Section 16B – Search & Discovery](#Section16b)  
[Section 17 – Direct Messaging & Conversations](#Section17)  
[Section 17B – Wireframe Callouts](#Section17)  
[Section 18 – Notifications & Messaging](#Section18a)  
[Section 18B – Notification Templates](#Section18b)  
[Section 20 – Admin Console](#Section20)  
[Section 21 – Engineering Runbooks, SRE, & SLOs](#Section21a)  
[Section 22 – Launch Plan & QA](#Section21a)  
[Section 23 – Support & Helpdesk UX](#Section23)  
[Section 24 – Payments Pipeline](#Section24)

**Section 0 — Vision & Policy Baseline**

**0.1 Product positioning (concise)**

* **Audience (Day‑1):** US‑only; **personal fundraisers** and **registered charities**.
* **Campaign beneficiaries:** **people** and **organizations**.
* **Content restrictions (initial):** forbid **weapons**, **adult content**, **raffles/lotteries**, and any illegal activity. (See 0.9 for the policy block.)
* **Experience tone:** warm, helpful, trust‑forward.

**0.2 Funding & goals**

* **Funding model:** *campaigner chooses* per campaign:
  + **Keep‑what‑you‑raise (KWR)** – funds paid out regardless of goal.
  + **All‑or‑Nothing (AoN)** – funds **only** paid out if goal is met by end date; otherwise donations are **automatically refunded by the system** (special policy exception; see refunds below).
* **Deadlines:** **required**. **Default 4 weeks**, **max 12 weeks**.
* **Goals:** **required** (no “goal‑less” campaigns).
* **Milestones & Stretch goals (decision made for you):** **Enabled** as optional *communication tools* (not gating payouts). Organizers can define milestones and “stretch goals” after the main goal is met. No effect on KWR/AoN mechanics.

**Acceptance criteria**

* AC‑FUND‑1: Campaign creation requires selecting **KWR** or **AoN**.
* AC‑FUND‑2: End date must be between **28–84 days** from start.
* AC‑FUND‑3: If AoN and goal not met at deadline → **system issues refunds automatically** to all donors; campaign status becomes **Not Funded**; progress archived.

**0.3 Donations & Pricing**

* **Donation type:** **one‑time** only (MVP).
* **Amounts:** custom **≥ $5**, **no max** (subject to processor limits).
* **Platform tip (decision made for you):** **Enabled**; suggested buttons **10% / 15% / 20%** + **Custom** + **No tip**. Preselect **15%**; persistent “No tip” visibly available.
  + Rationale: covers ops while keeping a $0 platform fee option for donors who prefer it.
* **“Cover fees” toggle (decision made for you):** **Enabled, default ON**. Shows estimated processing fees; donor may **uncheck**. If unchecked, processing fees reduce the **net to campaign**.
* **Anonymity & identity settings:**
  + **Hide my name publicly** (still share info with organizer; **rewards allowed**).
  + **Donate anonymously** (no contact details shared; **no rewards**; appears grey in organizer reward table).
* **Dedications & donor message:** **Enabled** by default; moderation applies.
* **Refund policy:**
  + **Organizer/Admin‑initiated refunds** permitted (per your rule).
  + **System‑initiated refunds** occur **only** for AoN campaigns that miss goal at deadline.
  + Tips: **refunded** when donation is system‑refunded; otherwise follow organizer/admin refund action.
* **Chargebacks:** platform disputes chargebacks with evidence (donation record, receipts, IP/device data, delivery of rewards if applicable).

**Acceptance criteria**

* AC‑DON‑1: Donation form shows **amount**, **tip selector**, **cover fees** toggle with clear fee math.
* AC‑DON‑2: Two separate privacy choices: **Hide name** vs **Donate anonymously** (with tooltips clarifying reward eligibility).
* AC‑DON‑3: Receipts show **gross**, **tip**, **fees**, **net to campaign**, and tax language.

**Microcopy**

* Tip explainer: “Your optional tip helps us keep platform fees low for everyone.”
* Cover fees: “Checked to help the campaign receive your full intended amount.”

**0.4 Payouts & cash‑out**

* **Who can receive funds (decision made for you):** **Single payout recipient per campaign**:
  + Personal campaigns → **Organizer**.
  + Charity/company campaigns → **Organization account** (EIN verified).
  + *(Designate a separate individual “beneficiary” payout added in Phase 2 to reduce Day‑1 complexity.)*
* **Payout timing:** **At campaign end** (both KWR and AoN that meet conditions).
* **Eligibility prerequisites:** **Verified email & phone**, **Driver’s License (or State ID)**, **verified payout account (bank)**, **minimum available balance** met.
* **Holds/reserves:** **3–5 business days** after campaign end (risk window).
* **Minimum payout amount (decision made for you):** **$50** per payout.
* **Maximum per payout/day (decision made for you):** **$50,000 per payout** and **$100,000 per day**; larger amounts require **Finance Ops** approval (admin override).
* **Failed payout:** notify organizer instantly; show status **Failed** with reason; **retry** daily for 5 days; provide **Replace payout method** CTA.

**Acceptance criteria**

* AC‑PAY‑1: “Cash out” button disabled until all eligibility checks pass.
* AC‑PAY‑2: Payout statement shows **gross donations**, **refunded**, **fees**, **net**, **hold window**, **ETA**.
* AC‑PAY‑3: On AoN miss → no payout event created.

**0.5 Identity, eligibility & age**

* **Age:** organizers must be **18+**.
* **KYC:** **DL/State ID required before campaign launch**; **SSN last‑4 required before payout**.
* **Charities/companies:** **EIN required**; business address; authorized representative attestation.
* **Geography:** **US‑only** (50 states + DC; include US territories if you want later—currently excluded for simplicity).

**0.6 Safety, moderation & trust**

* **Monitoring:** **Post‑publication** monitoring + **Report** flow (donors only).
* **Comments:** **Donors‑only** (can be turned off per campaign).
* **Donor Protection Guarantee:** If the platform confirms **proven fraud**, donations are refunded (net of irreversible processor fees if applicable).
* **Report reasons (decision made for you):**
  1. Fraud or misrepresentation
  2. Prohibited content or cause (weapons, adult, raffles/lotteries, illegal)
  3. Hate, harassment, or discrimination
  4. Privacy or impersonation concerns
  5. Spam or scams
  6. Misinformation or unsafe medical claims
  7. Other (free text)
  8. Reports create a **Trust & Safety case** with SLA targets.

**Acceptance criteria**

* AC‑SAFE‑1: “Report this campaign” visible to logged‑in donors; includes reason dropdown + details; shows confirmation.
* AC‑SAFE‑2: Campaign can be **suspended** by Moderation; donations disabled; public banner explains status.

**0.7 Brand, accessibility & auth**

* **Brand tone:** warm/helpful.
* **Accessibility (decision made for you):** target **WCAG 2.2 AA**.
* **Time/currency:** localize time to viewer; **USD** only.
* **Auth:** Phone‑first OTP + email verify; **Apple/Google sign‑in on Day‑1**.

**0.8 Communications & notifications**

* **Channels:** **Email + SMS**; OTP SMS has **voice fallback**.
* **Receipts include:** amount, tip, fees, net to campaign, AoN/KWR label, tax language (see below).
* **Organizer coaching:** enabled (e.g., “Add a feature image,” “Post an update,” “Thank your donors”).

**Key notification events (initial)**

* Registration: OTP sent; email verify sent → verified.
* Donation: success receipt to donor; new donation alert to organizer.
* Reward: organizer status change (Pending/Processed) → donor notified (email + SMS).
* Verification: each item verified/failed.
* Payouts: initiated, paid, failed (with reason).
* AoN result: funded vs not funded (refunds issued).

**0.9 Policies for public pages (summaries)**

**Restricted & prohibited categories (Day‑1)**

* Weapons, explosives, adult sexual content/services, raffles/lotteries, illegal activity, hate/terrorism, doxxing/harassment, fraud, misinformation (esp. medical), illicit drugs.
* **Review‑first** bucket (manual review may be required): political causes, legal defense, medical treatments with safety risks, crypto‑based rewards/funding.

**Refunds (public‑facing)**

* Organizer/Admin may refund donations; AoN not met → system refunds automatically. Tips refunded when donation is refunded.

**Tax language for receipts**

* “Donations to **personal** campaigns are **not tax‑deductible**. Donations to **verified charitable organizations** may be tax‑deductible; consult your tax advisor.”

**0.10 Discovery, SEO & growth**

**Discovery**

* Public browse by: **Category**, **Location**, **Verified‑only**, **Goal progress**, **Newly launched**, **Ending soon**, **Most raised**.
* Team campaigns: show **team leaderboard** on campaign page (optional toggle).

**Open Graph & social (decision made for you)**

* Dynamic **OG image** per campaign (cover image, campaign title, verified star, progress bar).
* **og:title**: “{Campaign Title} – Help {Organizer/Beneficiary} on {Brand}” (≤ 60 chars ideal).
* **og:description**: first 160 chars of short description.
* **twitter:card**: summary\_large\_image.
* Auto‑generated **share text** templates with tokens (title, short URL, hashtag).

**Referral links (your request)**

* Portal page “**Share & Referrals**” with:
  + **Personalized campaign link** + copy button
  + **Team member referral link** (if team mode; attributes donations to member)
  + One‑click share buttons for **Facebook, Instagram, X/Twitter, LinkedIn** (opens native share with prefilled text + OG)
  + **UTM tagging** (utm\_source, utm\_medium, utm\_campaign, utm\_content=team\_member\_id)
  + Mini performance panel: visits, conversions, $ raised per channel/member

**0.11 Support & Knowledge Base**

**Channels**

* **Form/email**, **phone**, and an **AI chatbot** backed by the KB.

**KB taxonomy (decision made for you)**

1. Getting Started (accounts, OTP, email verify)
2. Donating (payments, anonymity, receipts, refunds)
3. Running a Campaign (creation wizard, visuals, stretch goals/milestones)
4. Rewards & Fulfillment (organizer tools, donor reward tracking)
5. Verification & Eligibility (DL, SSN, EIN)
6. Payouts & Taxes (eligibility, timing, statements, failures)
7. Policies & Safety (prohibited uses, donor protection, reporting)
8. Troubleshooting (OTP not received, payment fails)
9. Team Fundraising (teams, links, leaderboards)
10. Analytics & Insights (organizer metrics)

**0.12 Metrics & Admin**

**Organizer Analytics (portal section you requested)**

* Donations over time; average donation; unique donors; top donors; conversion from visits→donations; source/UTM performance; reward tier uptake; refund rate; geography by state; device breakdown; team leaderboard (if applicable).
* Export CSV (donations, donors with consent, rewards status).

**Platform KPIs (north‑star & inputs; decision made for you)**

* North‑star: **Donations processed per active campaign per week**.
* Inputs: **Campaign conversion rate (visit→donation)**, **time to first donation**, **KYC pass rate**, **refund rate**, **payout failure rate**, **share→visit conversion**.

**Admin roles (decision made for you)**

* **Super Admin** – full access, audit.
* **Moderator (Trust & Safety)** – content flags, suspensions.
* **Compliance/KYC Analyst** – verification review, overrides.
* **Finance Ops** – payouts, refunds, statements, disputes.
* **Support Agent** – view users/campaigns, issue credits/refunds (within policy), respond to tickets.
* **Content/KB Editor** – manage KB and site copy.

**Day‑1 reports (decision made for you)**

1. Daily donations summary (gross, fees, tips, net; by category).
2. Active campaigns with goal, raised, days left; AoN/KWR split.
3. Payouts due this week (status, holds, failures).
4. Refunds issued (by reason, initiator).
5. Disputes/chargebacks pipeline.
6. KYC status funnel (pass/fail/pending, time to verify).
7. Trust & Safety queue (age by SLA).
8. Traffic & conversion (by source/UTM).
9. Reward fulfillment status (per campaign, roll‑up).
10. Top campaigns & categories (periodic ranking).

**0.13 MVP vs. Phase‑2**

**MVP (Day‑1 scope)**

* US‑only; phone‑first OTP + email verify; Apple/Google sign‑in
* Profile (email/phone change flows; avatar crop)
* Wallet (payment methods via Stripe)
* Verification: Email, Phone, **DL/State ID**, **SSN last‑4**, **EIN** (for orgs)
* Campaign creation wizard (Info, Details, Visuals, **optional Reward Tiers**)
* Public campaign page (gallery, story, FAQ, progress, donate)
* Donation flow (tips, cover fees, hide name vs anonymous, dedications)
* **Team fundraising (basic)**: opt‑in, team invite, member pages, **one payout to campaign**
* Rewards: organizer fulfillment table + donor rewards page
* Payouts: **at campaign end**, holds 3–5 business days, min $50
* Discovery: browse/search with core facets; dynamic OG; share/referral builder page
* Notifications: essential events (donation, reward, verification, payout, AoN result)
* Support: form/email, phone, chatbot; Knowledge Base
* Admin console: roles above; core reports

**Phase‑2**

* Recurring donations; comments moderation tools; organizer updates feed; beneficiary payout path; advanced fraud/risk scoring; saved searches & alerts; richer team competition features; gift cards; multi‑currency; mobile apps; deeper analytics dashboards; webhooks/integrations for charities; donor accounts merging.

**0.14 Practical constraints & guiding principles**

* **Compliance & privacy first:** KYC, age gating, US‑only data flows; minimize PII retention.
* **Accessibility:** build to **WCAG 2.2 AA** patterns from the wireframe stage.
* **Trust by default:** clear fee breakdowns; verified badges; report flow.
* **Operational simplicity:** one payout recipient per campaign for MVP; AoN auto‑refunds are system‑managed.

**0.15 Integrations**

* **Payments & Payouts:** Stripe (with Connect for payouts).
* **SMS/Voice:** Twilio (OTP + voice fallback).
* **Email:** SendGrid / Postmark / AWS SES (pick one).
* **Storage & media:** AWS S3 + image/video optimization via Cloudinary or Imgix.
* **Address validation:** USPS or Smarty (for US addresses).
* **Captcha/abuse:** hCaptcha or reCAPTCHA.
* **Analytics:** GA4 + Amplitude or PostHog (event analytics); Segment optional.
* **Search:** Algolia or Typesense (for fast search/facets).
* **Fraud signals (Phase‑2):** Sift / Kount / IP intelligence.
* **Helpdesk & chatbot:** Zendesk/Intercom/Freshdesk + chatbot powered by your KB.
* **Link shortener / OG image service:** internal or third‑party (e.g., ImageKit/Thumbor for dynamic OG).

# Section 1 — Product Vision, Personas & Journeys

**Scope:** Vision & principles, value proposition & non‑goals, detailed personas (public + staff), role capability summary (aligned with §3), end‑to‑end journeys with step‑by‑step AC, instrumentation, microcopy, risks, and a phased roadmap.  
**Depends on:** §0 (Foundations), §3 (Roles & Permissions), §4 (UX/A11y), §7 (APIs), §8 (Schema), §9 (CMS), §10 (Portal), §11 (KYC/KYB), §12–16 (Campaign/Discovery/Checkout), §18 (Notifications), §20 (Admin), §21–22 (Ops & Launch).

## 

## 1.0 Vision, value & guardrails

**Vision (US‑only MVP):**  
Make it **trustworthy**, **simple**, and **fast** to raise and give money for personal causes and registered charities—backed by strong identity checks, clear rules, fair refunds, and excellent organizer tooling.

**Value promises (externally visible):**

1. **Fast to launch** — verified organizers can publish in ~minutes (after ID).
2. **Fast to donate** — minimal friction, clear fees, private options (hide name or anonymous).
3. **Safe for all** — strong KYC/KYB, risk controls, donor‑only reporting, transparent AoN/KWR.
4. **Reward‑ready** — optional, simple tier rewards with tracking & nudges.
5. **Team power** — attribution links and leaderboards, without payout complexity.

**Non‑goals (MVP):**

* No recurring donations, crypto, multi‑currency, or international payouts.
* No public comments; no open marketplace for merch.
* No guest checkout (donations require account, per §14.A.2).
* No organizer self‑service for custom payout schedules (payouts are at campaign end, per §15/§2).

**Product principles (internal):**

* **Trust by default:** decisions tilt toward safety; copy is clear about rules.
* **Clarity of money:** always show where every dollar goes.
* **Accessibility before aesthetics:** WCAG 2.2 AA enforced (§4).
* **Few, strong opinions:** keep choices minimal (e.g., 6 reward tiers max; whole‑dollar donations).
* **Audit everywhere:** admin/staff actions, risk decisions, payouts.

## 1.1 Personas (deep profiles)

Each persona includes: goals, common tasks, blockers, device bias, accessibility, and success signals. Role abilities reference §3.

### P1 — ****Donor**** (individual supporter)

* **Goals:** give quickly/safely; optionally remain private; track rewards and receipts.
* **Top tasks:** find campaign, donate, claim reward, download receipt, message organizer if needed.
* **Blockers:** confusing fees/tips; distrust; slow 3DS; complex forms; unclear reward status.
* **Devices:** 70% mobile, 30% desktop (assumption; instrument in §20.T).
* **A11y:** large tap targets, high contrast, voice‑over labels, keyboardable checkout.
* **Success signals:** donation completion rate, checkout P95 ≤ 4s, reward claim completion, low refund requests.

### P2 — ****Organizer (Individual)**** (default campaign owner)

* **Goals:** launch a compliant, attractive campaign; invite team; fulfill rewards; get paid on time.
* **Top tasks:** verify ID, create campaign/story/media, set tiers, publish, manage team, fulfill rewards, request payout.
* **Blockers:** KYC friction; media prep; unclear payout holds; managing addresses/tracking.
* **A11y:** form validation clarity, structured WYSIWYG, drag‑drop upload with keyboard controls.
* **Success signals:** time‑to‑publish, donations in first 72h, fulfillment SLA, payout success.

### P3 — ****Org Admin (Nonprofit/Company)****

* **Goals:** EIN verification, multiple campaigns, exportable reports, team delegation.
* **Top tasks:** org profile, staff roles, campaigns oversight, payout compliance.
* **Blockers:** EIN mismatches; board approvals; finance reconciliation.
* **Success signals:** verified nonprofit badge, payout reconciliation accuracy, staff productivity.

### P4 — ****Team Lead / Co‑Lead / Member**** (campaign‑specific roles)

* **Goals:** share links, raise funds credited to them; see leaderboard.
* **Top tasks:** accept invite, get referral link, share, monitor personal tally.
* **Blockers:** invite expiration; attribution doubts; COI rules confusion.
* **Success signals:** link CTR→donation rate; member satisfaction; minimal COI blocks.

### P5 — ****Campaign Support**** (organizer‑appointed helper)

* **Goals:** assist with rewards & donor comms; no money control.
* **Top tasks:** view reward table, update statuses, add tracking, reply to donor DMs.
* **Blockers:** unclear permissions.
* **Success signals:** on‑time fulfillment; fewer donor tickets.

### Staff personas (internal)

* **Moderator (Trust & Safety):** triage reports, require edits, suspend/unsuspend; SLA compliance.
* **Risk Analyst:** review high‑risk donations, adjust rules/lists; chargeback rate.
* **Finance Ops:** payout queues, returns, reserves; reconciliation accuracy.
* **Support Agent:** helpdesk integration, macros, ticket SLAs.
* **Super Admin:** feature flags, templates, SEO/ranking knobs; minimal hotfixes.

## 1.2 Role capability snapshot (tie‑in to §3)

| **Capability** | **Donor** | **Organizer** | **Org Admin** | **Team Lead** | **Co‑Lead** | **Member** | **Campaign Support** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Donate to a campaign | ✅ | ✅ (self allowed, flagged) | ✅ | ❌ (blocked on own campaign) | ❌ | ❌ | ✅ (to other campaigns only) |
| Create/publish campaign | ✅ (after KYC gate) | ✅ | ✅ (org campaigns) | ❌ | ❌ | ❌ | ❌ |
| Manage team | — | ✅ | ✅ (org‑wide) | ✅ | ✅ (limited) | ❌ | ❌ |
| Rewards fulfillment | — | ✅ | ✅ | — | — | — | ✅ |
| Request payout | — | ✅ | ✅ | — | — | — | — |
| Direct messaging | ✅ | ✅ | ✅ | ✅ | ✅ | ✅ | ✅ (reward context) |

Full permissions matrix lives in §3. This table ensures journey steps below align with actual powers.

## 1.3 Primary journeys (end‑to‑end, with acceptance criteria & event instrumentation)

### J1 — ****Donor: discover → donate → reward → receipt****

**Steps & AC**

1. **Discover** (Home/Search/Category/Profile; §16)
   * AC: Search facets/“Trending/Ending soon” available; Suspended campaigns hidden.
   * Events: home\_view, search\_query, campaign\_card\_click.
2. **Campaign page** (§13)
   * AC: clear progress, AoN chip if applicable, sticky donate; team leaderboard optional.
   * Events: campaign\_page\_view, donate\_cta\_click.
3. **Donate widget & checkout** (§14)
   * AC: amount ≥ $5, whole dollars; tip control; cover‑fees toggle; terms checkbox required; COI block enforced.
   * AC: 3DS flows recover; retry once on fail; non‑US card allowed with extra screening.
   * Events: donate\_amount\_preset\_click, donate\_other\_amount\_focus, checkout\_start, checkout\_success|fail.
4. **Confirmation & receipt** (§18)
   * AC: email receipt within 5 min; in‑app notification; AoN text if relevant.
   * Events: donation\_receipt\_delivered, inapp\_notification\_open.
5. **Reward claim (if tier met)** (§12.D)
   * AC: claim/opt‑out/anonymous logic; address validation; edit until Pending. Persistent “Finish claim” banner if abandoned.
   * Events: reward\_claim\_open|submit|opt\_out, address\_validate\_success|fail.
6. **DM (optional)** (§17/§10.S)
   * AC: DM respects organizer policy (Anyone/Donors‑only/Off); mute/report available.
   * Events: dm\_thread\_start, dm\_message\_send, dm\_report.

**Success definition (J1):** End‑to‑end conversion ≥ industry baseline; reward claim completion ≥ 80% for physical rewards; refund requests ≤ target.

### J2 — ****Organizer: register → verify → build → publish → manage → payout****

**Steps & AC**

1. **Registration & security** (§10.A, §11)
   * AC: phone OTP; email verify; 18+ gate; DL/ID before publish; SSN last‑4 before payout.
   * Events: register\_start|complete, kyc\_start|pass|fail.
2. **Create campaign** (wizard; §12)
   * AC: category, goal ≥ $100, 4–12 week deadline; city/state US; story/FAQ; media quotas; reward tiers ascending; review & publish gate.
   * Events: campaign\_create\_step\_{n}\_view|complete, campaign\_publish.
3. **Team** (§12.J)
   * AC: invite via single‑use link; ≤5 seats including Lead; leaderboard toggle.
   * Events: team\_invite\_send|accept, leaderboard\_toggle.
4. **Live management**
   * AC: updates (1/day), reward fulfillment table, donor DMs, moderation compliance if reports arrive.
   * Events: update\_post, reward\_status\_bulk\_update, dm\_reply.
5. **End → payout** (§15/§20.D)
   * AC: 3–5 business day hold; eligibility checks; payout requested/approved/paid; returns retried after bank update; statements downloadable.
   * Events: payout\_request|approved|paid|returned.

**Success (J2):** Time‑to‑publish median (from registration complete) ≤ target; payout paid within SLA; low support volume.

### J3 — ****Org Admin (nonprofit): org setup → EIN → campaigns → reporting****

**Steps & AC**

1. **Org profile & KYB** (§11)
   * AC: EIN verified → nonprofit badge; staff roles (admin/support) assigned.
   * Events: org\_create, ein\_verify\_pass|fail.
2. **Campaign oversight**
   * AC: view/approve multiple campaigns; export donations; role bindings visible.
   * Events: org\_campaign\_export, org\_role\_assign.
3. **Finance**
   * AC: payouts to org account; returned payouts resolved; audit logs present.
   * Events: payout\_case\_update, audit\_view.

### J4 — ****Team fundraising: invite → share → attribute → leaderboard****

**Steps & AC**

1. **Invite & accept** (§12.J)
   * AC: single‑use token; expires 7 days; seat cap respected.
   * Events: team\_invite\_send|accept.
2. **Share & attribute**
   * AC: each member ref link; attribution persists to checkout; refunds reduce totals.
   * Events: ref\_link\_copy, ref\_donation\_attributed.
3. **Leaderboard**
   * AC: public module shows correct totals; can toggle off.
   * Events: leaderboard\_view, leaderboard\_toggle.

### J5 — ****Staff: report → review → decision**** (Trust & Safety)

**Steps & AC**

1. **Report** (donors‑only; §13.10)
   * AC: reasons list, attachments; creates mod case; organizer not notified of raw report.
   * Events: report\_submit.
2. **Moderation** (§20.B)
   * AC: evidence view, actions (soft warning, suspend, require edits); SLA timers.
   * Events: mod\_case\_open|decision.
3. **Outcome comms** (§18)
   * AC: templated emails; public page reflects changes (suspended banner).
   * Events: mod\_notification\_sent.

## 1.4 Journey wires & UX notes (for design)

* **Discover → Campaign page**: ensure card → page handoff retains **member ref=** so attribution survives (UTM propagation).
* **Donate sheet (mobile)**: bottom sheet with quick chips + custom amount + tip/cover fees; CTA pushes to §14 flow.
* **Reward claim page**: wizard with delivery type conditional; address autocomplete; “Finish later” persists banner in portal.
* **Organizer wizard**: progress breadcrumbs; review page summarizing readiness checklist.
* **Team overview**: cards for each member (raised amount, donations count, last donation time) + share/referral controls.
* **Moderation**: case timeline with actions audit; preview public page vs suspended view.

(Visual wires will reference existing UI kits—this spec names modules, states, and AC so design/dev can produce consistent screens.)

## 1.5 Instrumentation map (events & properties)

All events flow to first‑party analytics (§8.L, §20.T). Include user\_id, session\_id, campaign\_id, role\_context (anon/donor/organizer/team/staff), ref\_code (if any), funding\_model, and usd\_amount where relevant.

**Key events:**

* **Discovery**: home\_view, search\_query{q,filters}, campaign\_card\_click{position}
* **Campaign**: campaign\_page\_view, share\_click{channel}, copy\_link
* **Checkout**: checkout\_start, checkout\_success|fail{code}, donate\_amount\_preset\_click{value}
* **Rewards**: reward\_claim\_open|submit|opt\_out, address\_validate\_success|fail
* **Team**: team\_invite\_send|accept, ref\_link\_copy, ref\_donation\_attributed
* **Organizer**: campaign\_create\_step\_{n}\_complete, campaign\_publish, update\_post
* **Finance**: payout\_request|approved|paid|returned
* **Moderation**: report\_submit, mod\_case\_open|decision
* **Messaging**: dm\_thread\_start, dm\_message\_send, dm\_report

**Dashboards (Section 20.T builder presets):**

* Funnels (Discover→Donate; Create→Publish), Reward Claim completion, Team attribution share, Payout SLA, Report SLAs, A11y Web Vitals.

## 1.6 Copy kit (persona‑specific, ready to use)

**Donor — donate guardrails**

* **Min error:** “Minimum donation is **$5**.”
* **Whole dollars:** “Enter a whole‑dollar amount.”
* **COI block:** “You’re part of this campaign’s team. Only the campaign owner can donate here.”
* **3DS step‑up:** “For your security, we’ll confirm this payment with your bank.”

**Organizer — publish/payout**

* **Publish gate:** “Almost there—verify your ID to publish.”
* **Payout hold:** “Funds will be available **3–5 business days** after your campaign ends.”

**Team**

* **Invite expired:** “This invite link has expired. Ask the team lead to send a new one.”

**Moderation**

* **Paused banner:** “This campaign is temporarily unavailable while we review a report.”

(Further microcopy lives inline in §12–14; this kit covers journey‑specific moments.)

## 1.7 Risks & mitigations (specific to this section)

| **Risk** | **Impact** | **Mitigation** |
| --- | --- | --- |
| Persona/role creep (journeys assume powers that roles don’t have) | Broken flows | Kept in lockstep with §3; capability table above; tests in §22 cover role gating |
| Referral attribution loss between pages | Lost team credit | Persist ref= through SSR/CSR; propagate to checkout; test in §22 |
| Reward claim abandonment | Donor dissatisfaction | Persistent banner; reminder notifications; simple claim form; address autocomplete |
| KYC drop‑off | Fewer campaigns | Tooltips, retry tips, selfie only when needed, optional live help |
| Copy drift vs policy | Legal exposure | §9.9 legal pages two‑person approval; copy library keys in §20.O |

## 1.8 Phased rollout & experiments

**MVP scope here:** everything documented in J1–J5 with current policies.  
**Phase‑2 candidates:** comments, push notifications, corporate matching, org‑level shared inbox enhancements, deep personalization.  
**Experiments (A/B ready):**

* Donation preset amounts set (chip set A vs B).
* Home module order (Trending vs Editor’s Picks first).
* Reward claim page layout (single vs two‑step address).
* Leaderboard visibility default (on vs off).  
  All experiments must define metrics in §20.Q and respect §4 performance budgets.

## 1.9 Acceptance Criteria (Section 1)

* **Personas**: defined with tasks, blockers, and a11y considerations; reflected in journeys.
* **Journeys**: J1–J5 steps map 1:1 to implemented modules; each step has AC and events.
* **Capabilities**: table aligns to §3; no journey step requires missing permission.
* **Instrumentation**: events list complete; dashboards can be built using §20.T builder.
* **Copy**: core microcopy included; consistent with §12–14 & §18.
* **Risks**: listed with mitigations; tests in §22 cover key risks (ref propagation, COI, KYC gates).

## 1.10 Artifacts to produce (design/dev tasks)

* Journey swimlanes (Donor, Organizer, Team, Staff) in design tool; export PNGs to CMS assets.
* Copy library keys for messages above (hook into §20.O).
* Analytics event contracts (TypeScript interfaces) for the events list.
* QA/UAT scripts derived from J1–J5 (append to §22 Appendix A).

# 

# Section 2 — Platform Economics, Pricing & Policy

**Scope:** How every dollar flows. Pricing knobs, fee math, cover‑fees algebra, tips, AoN vs KWR economics, refunds/chargebacks, reserves & payout timing, accounting/ledger effects, statements/receipts, admin controls, copy, edge cases, and acceptance criteria.  
**Depends on:** §0 (Foundations), §3 (Roles), §5 (Risk), §7 (APIs/Stripe), §8 (DB), §10 (Portal), §12–15 (Campaign/Rewards/Checkout/Payouts), §18 (Notifications), §20 (Admin), §21–22 (Ops/QA).  
**Assumptions:** US‑only, USD‑only. Payments via Stripe (card rails incl. Apple/Google Pay/Link). Whole‑dollar donations (no cents), minimum $5. Tips and “cover fees” available per §14 decisions.

## 2.0 Definitions & units

* **Donation (D):** Whole‑dollar amount the donor intends to give to the **campaign** (≥ $5).
* **Tip (T):** Optional donor gratuity to the **platform** (configurable presets).
* **Cover‑fees amount (CF):** Extra amount added so the **donor** covers processor fees. Credited to the **campaign**.
* **Gross charge (G):** Total the donor is charged: G = D + T + CF.
* **Processor fees (F):** Fees charged by processor on **G** (e.g., percent p + fixed fee f). May include surcharges (international/cross‑border).
* **Net to campaign (N):** What the campaign accrues before reserves/holds.
* **Reserve:** % of net held for X days post‑campaign end (risk‑based).
* **Wallet balance:** Organizer’s available balance = sum of nets − refunds − prior payouts − reserves − chargebacks.

All monetary storage: **cents (int)**; display with $.

## 2.1 Admin‑config pricing knobs (20.I)

**Global (defaults for MVP; adjustable in Admin):**

1. **Processor fee model:** p% + f (percent + fixed cents). (Example defaults for modeling: *p = 2.9%*, *f = $0.30*)
2. **International surcharge (optional):** extra % if card BIN is non‑US. (default 0)
3. **Nonprofit reduced fees:** toggle + rate set (if Stripe nonprofit rates arranged). (default OFF)
4. **Cover fees:**
   * **Enabled:** **YES**
   * **Behavior:** **Cover entire processor fee on G** (recommended) or **Cover donation‑only share** (toggle). (default: entire fee)
   * **Default state:** **Unchecked** (donor must opt‑in).
   * **Rounding:** to **nearest cent** (UI shows preview).
5. **Tip control:** **ON** with presets **0% / 10% / 15% / Custom**. Pre‑selected suggestion = **10%** (mobile‑optimized copy; editable).
6. **Refund fee policy:** who absorbs **non‑returned** processor fees on refunds:
   * Organizer‑initiated → **Organizer** (default).
   * Admin goodwill → **Platform decides** per refund (toggle in modal).
   * AoN auto‑refunds → **Platform absorbs residual fees** by default (donor gets full amount back).
   * **Tips on refunds:** AoN not‑funded → **Refund tips TOO (default ON)**; Organizer/Admin manual refunds → **Tips NOT refunded (default OFF)** with override.
7. **High‑amount manual review threshold:** donations **≥ $10,000** → accept & **hold for review** (payout‑locked).
8. **Payout thresholds:**
   * **Minimum payout amount:** **$50** (from §15.2.4),
   * **Timing:** **On campaign end** + **3–5 business days** hold (configurable window).
   * **Dual‑approval for payouts ≥ $50,000** (20.D).
9. **Reserves:** risk‑based **0–20%** for **30–60 days** (Section 5.8). Defaults: **0%** (low risk), **10%** (elevated), **20%** (high).
10. **Rounding policy in UI math:** show **sample math** on hover; totals exact to the cent on confirmation (§14.C.13).

## 2.2 Fee math (formalized) & algorithms

This is the source of truth for checkout, receipts, wallet accruals, and statements.

### 2.2.1 Processor fee function

F = p \* G + f + s \* G  
Where:

* p = base percent fee; f = fixed fee;
* s = surcharge percent (international/cross‑border) (usually 0).
* G = D + T + CF.

### 2.2.2 ****Cover entire fee**** (default behavior)

Goal: donor covers **all** processor fees so **N = D** and platform receives **full T**.

Solve **CF** such that CF = F:

CF = ( (p + s) \* (D + T) + f ) / (1 - (p + s))

G = D + T + CF

F = (p + s) \* G + f ≈ CF (subject to rounding to cents)

N = (D + CF) - F = D

**Rounding:** Compute CF in cents with ceiling to nearest cent to ensure N ≥ D by ≤ $0.01. UI shows: “We’ll add **$x.xx** to cover fees.”

### 2.2.3 ****Cover donation‑only share**** (alternate toggle)

Goal: donor covers fees attributable to **D** only; platform tip **T** absorbs its own fees.

Let F\_total = p\*G + f + s\*G

Pro‑rate to donation: F\_D = F\_total \* (D / (D + T))

Set CF = F\_D / (1 - p - s) (approx, iteratively refine with 1–2 steps)

N ≈ D

Platform tip net ≈ T - (F\_total - F\_D)

We keep the default “Cover entire fee” because it’s simpler to explain and preserves full tip.

### 2.2.4 No cover‑fees (donor didn’t opt‑in)

* CF = 0
* F = p \* (D + T) + f + s \* (D + T)
* Fees are **allocated pro‑rata** between **campaign (D)** and **tip (T)**:

F\_D = F \* (D / (D + T unless T=0 → 1.0))

F\_T = F - F\_D

N = D - F\_D

Platform tip net = T - F\_T

### 2.2.5 Worked examples (using p=2.9%, f=$0.30, s=0; rounded to cents)

1. **$50 donation, no tip, Cover Fees ON (entire fee)**
   * D=50, T=0
   * CF = (0.029\*(50) + 0.30) / (1 - 0.029) = 1.75 / 0.971 ≈ $1.80
   * **G = $51.80**; **F ≈ $1.80**; **N = $50.00**.
2. **$50 donation, 10% tip ($5), Cover Fees ON (entire fee)**
   * D=50, T=5
   * CF = (0.029\*(55) + 0.30) / 0.971 ≈ $1.95
   * **G = $56.95**; **F ≈ $1.95**; **N = $50.00**; **Platform tip net = $5.00**.
3. **$50 donation, $5 tip, Cover Fees OFF**
   * G = 55; F = 0.029\*55 + 0.30 = $1.90
   * Pro‑rate fee to D: F\_D = 1.90\*(50/55) ≈ $1.73; **N ≈ $48.27**
   * Pro‑rate fee to T: F\_T = $0.17; **Tip net ≈ $4.83**.
4. **$5 minimum donation, 10% tip ($0.50), Cover Fees ON (entire)**
   * CF = (0.029\*(5.5) + 0.30)/0.971 ≈ $0.47
   * **G ≈ $5.97**, **F ≈ $0.47**, **N = $5.00**, **Tip net = $0.50**.

Edge (international surcharge example with *s=1%*) is supported by the same formula; UI shows “includes additional card processing costs.”

## 2.3 AoN vs KWR economics

* **KWR (Keep‑What‑Raised):** Donations are final unless organizer/admin refunds. N accrues immediately.
* **AoN (All‑or‑Nothing):** We **charge now**. If the goal is **not** met by deadline → **auto‑refund** donations.
  + **Auto‑refund economics:**
    - Donor receives **full donation back**.
    - **Tips:** **Refunded by default** for AoN failures (Admin‑configurable).
    - Any processor fee losses are **platform‑absorbed** (donor should be made whole).
    - Team attributions and public page show “Not funded — all donations refunded.”

**AC‑AoN‑1:** When AoN fails, donation rows flip to aon\_auto\_refunded, organizer N is decremented to **0** for that campaign.

## 2.4 Refunds policy & money flow

**Who can refund:** Organizer (their donations), Admin (any donation).  
**Windows:** See §14.L (policy defined); system always allows partial or full refunds.

**Execution flow:**

1. **Pre‑payout refund:** reduce N and **wallet** immediately after refund webhook.
2. **Post‑payout refund:** create **negative balance**; recovered from future campaign nets/payouts. If organizer exits, escalate to **collections** workflow (admin case, optional dunning).

**Fees on refunds (provider may not return F):**

* **Organizer‑initiated:** non‑returned fees are **organizer’s cost** (wallet reduced / negative balance).
* **Admin goodwill:** toggle “Platform absorbs fees” individually.
* **AoN auto‑refund:** platform absorbs residual fees; donor fully refunded.
* **Tips on refund:**
  + AoN not funded → **refunded** (default).
  + Organizer/Admin discretionary → **not refunded** (default), with override.

**Partial refunds:**

* Recompute and store refund.amount\_cents; update receipt; adjust N and wallet; **pro‑rate fee allocation** proportionally.

**AC‑REF‑1:** Refunds **never** over‑refund beyond paid amount; tips and donation components tracked distinctly in receipt.  
**AC‑REF‑2:** Negative balances are visible in Wallet with actions and recovery rules.

## 2.5 Chargebacks (disputes) economics

* **When opened:** place a **hold** on the disputed donation amount against the organizer’s wallet (if not already paid out) or create/extend **negative balance** if post‑payout.
* **Won:** release hold.
* **Lost:** deduct disputed amount **+ dispute fee** from organizer wallet/negative balance.
* **Tips:** disputed and lost → donor refunded in full; tip considered part of the disputed charge and reversed; platform bears its share unless Goodwill pool is configured.

**AC‑CB‑1:** Dispute outcomes reconcile with Stripe webhooks; wallet and statements reflect changes same‑day.

## 2.6 Payout timing, reserves & statements

* **Schedule:** Payout **on campaign end** if:
  + Identity verified (email/phone/ID), SSN/EIN verified, bank verified;
  + **Minimum payout** (≥ $50) met;
  + No **compliance hold**;
  + **Hold window** (3–5 business days) passed.
* **Reserves:** risk‑based percentage held until release\_at.
* **Returns:** If payout **returned** → funds go back to wallet; organizer notified (email+SMS+voice fallback) and prompted to update bank; Finance can **resubmit** with audit trail (20.D).

**Organizer statements (downloadable)**

* Columns: Period, Gross donations, Refunds, Chargebacks (net), Processor fees (informational), Reserves in/out, Net available, Payouts, Ending balance.
* Each **payout** includes an itemized list of donations included (20.D).

**AC‑PO‑1:** Statement totals reconcile to wallet movements.  
**AC‑PO‑2:** Returned payouts preserve original payout record with a linked **return** entry and new **resubmission** entry.

## 2.7 Accounting & ledger (operational model)

(High‑level, implementation may be simplified but must preserve invariants.)

**On donation succeeded:**

* Credit **Campaign Accrual** by N (computed using chosen cover‑fees model).
* Credit **Platform Revenue (Tips)** by tip net (if cover entire fee, tip net = T; else T - F\_T).
* Record **Processor Fees (memo)** from balance transaction for reconciliation (not expensed per donation if Connect handles pass‑through).

**On refund:**

* Reverse entries proportionally; if post‑payout → create **negative balance** (liability).

**On payout paid:**

* Debit **Wallet**; record **Payout** with memo and destination token.

**AC‑LG‑1:** Sum of donation net − refunds − payouts − holds = **wallet ending balance** at any time.

## 2.8 Receipts & donor/organizer displays

**Donor receipt (email + portal):**

* Line items: Donation, Tip (if any), Cover fees (if any).
* If AoN: “Charged now; automatically refunded if the goal isn’t met by {date}.”
* If refund/partial: updated receipt with **Refund amount** and **Remaining donation** (if partial).
* Tax advisory: **“Donations to individuals are generally not tax‑deductible. Donations to verified nonprofits may be.”** (links to KB).
* Show **donor privacy** choice (“Name hidden publicly” or “Anonymous donation”).

**Organizer portal:**

* Real‑time **Net to campaign** (sum of N)
* **Refunds/chargebacks** table
* **Wallet** with **Available / On hold / Reserved**
* **Payouts** with statuses and statements

**AC‑REC‑1:** Numbers on checkout, confirmation, and receipt match to the cent.  
**AC‑REC‑2:** Donor can download a **year‑to‑date** donations CSV (14.K.41–43).

## 2.9 UI copy (ready to ship)

**Checkout fee math tooltip (Cover ON):**  
“**Cover fees** adds a small amount so the organizer receives your full donation after processing costs.”

**Checkout fee math tooltip (Cover OFF):**  
“Processing costs are deducted from your donation and any tip. You can choose to cover them.”

**Tip explainer:**  
“Tips help us run the platform. Optional and appreciated.”

**AoN explainer (header chip & checkout):**  
“**All‑or‑Nothing:** Charged now; automatically refunded if the goal isn’t met by {date}.”

**Refund outcomes (donor):**  
“Your **${amount}** refund has been processed. You’ll see it on your statement within 5–10 business days.”

**Payout returned (organizer):**  
“We couldn’t deliver your payout for **{campaign}**. Please update your bank details to try again.”

## 2.10 Admin Console controls (20.I / 20.D / 20.H)

* **Pricing panel:** set p, f, s; nonprofit rate; toggle **cover‑fees behavior** (entire vs donation‑only); edit **tip presets & default**.
* **Refund policy panel:** defaults for **refund fees absorption** and **tips‑on‑refund** (AoN vs Organizer/Admin).
* **Payouts panel:** min payout, hold window, dual‑approval threshold, reserve presets.
* **Economics report:** daily aggregation (gross, tips, fees (memo), refunds, chargebacks, reserves, net, payouts) with CSV export.
* **What‑if simulator:** enter D/T and see outcomes under current config for transparency and support.

**AC‑ADM‑1:** Any pricing change is **audited** (who/what/when) and **effective timestamped**; receipts/ledger reference **the config in effect at time of donation**.

## 2.11 Edge cases & rules

* **Donation below min ($5):** hard block with friendly copy; express chips respect min.
* **Cover fees rounding:** if rounding causes N > D by $0.01, we still show “Organizer receives $D” and carry 1¢ remainder into platform “Adjustment” line to avoid confusion.
* **Goal increase (KWR only)**: allowed upward once; no effect on prior donations economics, but copy shows “Goal updated on {date}.”
* **Campaign suspended:** donations disabled; no accruals; refunds possible for recent donations as policy.
* **Post‑payout refunds causing large negative balance:** payouts blocked across organizer’s account until cleared; Finance Ops case created.
* **International cards (if allowed):** surcharge configured; risk engine may add step‑ups (Section 5).
* **Charge splitting:** Never split a single donation across multiple payouts; ensure each donation belongs to **exactly one** payout.

## 2.12 Data model bindings (to §8)

* donation.donation: amount\_cents, tip\_cents, fee\_cents, net\_to\_campaign\_cents, funding\_model\_snapshot, status.
* finance.refund: amount\_cents, tip\_refunded\_cents (new field), fee\_policy (enum).
* finance.wallet: balances (available/on\_hold/reserved).
* finance.payout & finance.payout\_item: snapshot of donations included.
* finance.reserve: percent, release\_at, reason\_code.
* analytics.event: checkout\_\*, payout\_\*, refund\_\*.

## 2.13 Acceptance Criteria (economics)

1. **Math correctness:** Given (D, T, config), computed (CF, F, N) satisfy chosen model to the cent; receipts and wallet reconcile.
2. **Cover fees ON:** Organizer **N = D** (±$0.01 due to rounding), platform gets full **T** under “cover entire fee” model.
3. **Cover fees OFF:** Fees are pro‑rated between donation and tip; displays show both.
4. **AoN failure:** Auto‑refund principal (and tips per default); organizer N resets; campaign marked Not Funded.
5. **Refunds:** Pre‑payout reduces accruals; post‑payout creates negative balance; policy for who absorbs fees honored.
6. **Chargebacks:** Holds/adjustments applied; outcomes update wallet and statements.
7. **Payouts:** Trigger only when eligibility met and hold window elapsed; reserve applied; returned payouts handled with resubmit.
8. **Admin changes:** Audited; do not retro‑change prior receipts; simulator reflects current config.
9. **Reports:** Daily economics report sums to ledger; CSV export available.

## 2.14 QA checklist (tie to §22)

* Unit tests: fee calculator (cover entire vs donation‑only), AoN auto‑refunds, partial refunds, pro‑rata fee allocation with tip.
* E2E: Donate with/without tip; toggle cover fees; verify organizer N, donor receipt lines; AoN failure batch refund; post‑payout refund negative balance; returned payout resubmit.
* Admin: flip knobs (tip defaults, cover model, min payout); confirm receipts use **historic** config; simulator accuracy.
* Reports: Economics report totals match DB queries; statements export equals wallet deltas.

## 2.15 Roadmap (Phase‑2)

* **ACH/Bank payments** (lower fees) with risk controls.
* **Corporate matching** prompts & employer search.
* **Localized pricing experiments** (different tip presets by category).
* **Per‑campaign fee sponsorship** (org covers card fees for donors).
* **Platform coupon/credit system** (promo offsets; not cash).

# 

# Section 3 — Role Assignment & Onboarding

## 3.A Objects & scope

* **RoleBinding** (already defined): ties a **user\_id** to a **role** with a **scope**
  + scope\_type: campaign | organization | global
  + scope\_id: campaign\_id / organization\_id / null
  + role: team\_lead | co\_lead | member | campaign\_support | org\_admin | org\_support | …
  + permissions[]: optional fine‑grained toggles (e.g., “export CSV”, “moderate comments”)
  + status: active | revoked | pending\_invite | expired\_invite
* **Organization**: created when a campaign chooses “organization/charity” and completes EIN verification (Section 11).
* **People directories**:
  + **Campaign → Team & Support**
  + **Organization → People**

**Principle:** A user can hold multiple RoleBindings. **Effective permissions = union** of bindings within the same scope (COI rules still apply).

## 3.B Admin surfaces (where roles are assigned)

### B1) Campaign → ****Team & Support**** (owned by Team Lead / Verified Organizer)

* **Tabs:**
  + **Members** (Lead / Co‑Lead / Members)
  + **Support** (Campaign Support seats)
  + **Invites** (pending, expired; resend/revoke)
  + **Settings** (leaderboard, description, photo)

**Actions:**

* **Invite Member** (email) → assign **Member** or **Co‑Lead** role
* **Invite Support** (email) → **Campaign Support** with optional permissions:
  + “View donor list” (off by default)
  + “Export CSV” (off by default)
  + “Moderate comments” (off by default)
* **Promote/Demote** between Member ↔ Co‑Lead (subject to seat limits)
* **Remove** user (revokes RoleBinding; preserves historical attribution)

### B2) Organization → ****People**** (owned by Org Admin)

* **Tabs:**
  + **Admins** (Org Admins)
  + **Support** (Org Support)
  + **Invites**
  + **Scopes** (assign which campaigns Org Support can access)

**Actions:**

* **Invite Org Admin** (email)
* **Invite Org Support** (email) with scope:
  + **All org campaigns** or **Select campaigns**
  + Optional permissions: “View donor list”, “Export CSV”, “Moderate comments”
* **Change scope** (add/remove campaigns)
* **Remove** user from org roles

**AC**

* AC‑SURF‑1: Both surfaces show **seat counters** (Team seats used; Support seats used).
* AC‑SURF‑2: Changes are **audited** with actor/time.

## 3.C Invitation lifecycle (new vs existing vs logged‑in users)

**Invite issuance**

* Admin enters **email** → system creates **single‑use token**, expiry **7 days** → sends email + (optional) SMS if known.
* Invite shows: role, scope, permissions, inviter name, expiry.

**Invite acceptance routes**

1. **Not registered**
   * Click invite → **Registration** (phone OTP, email verify auto‑confirmed from invite email) → set password → **Accept role** → redirected to the correct dashboard (Campaign or Org).
   * **Email must match** the invite email.
2. **Registered but logged out**
   * Click invite → **Login** (email prefilled from invite) → **Accept role** → redirect.
3. **Already logged‑in**
   * If **logged‑in email matches invite email** → one‑click **Accept role**, session refresh → redirect.
   * If **logged‑in email differs** → show **Switch account** modal:
     + **Option A:** Log out and sign in as **{invite email}**.
     + **Option B:** Request inviter to **resend invite** to current account email (button opens draft email to inviter).
     + **Security default:** **Email must match** to accept (prevents accidental assignment to the wrong user).
     + (Admin override via Admin Console exists; see 3.G.)

**Expired/revoked**

* Expired → show “Invite expired” with **Request new invite** button (notifies inviter).
* Revoked → show “Invite revoked by {inviter}” with no action.

**AC**

* AC‑INV‑3: Acceptance **requires matching email**; otherwise block with Switch‑account flow.
* AC‑INV‑4: Token is single‑use; consuming it activates RoleBinding and invalidates the token.

## 3.D Role change while user is online (session updates)

* **Immediate effect:** On the next API call (≤ a few seconds), we **refresh effective roles**.
* **UI feedback:** show toast “Your access has changed. Please refresh if something looks off.”
* **Sensitive downgrades** (e.g., removing access that reveals donor contact): force **session refresh** and re‑auth if needed.

**AC**

* AC‑LIVE‑1: Role updates reflect without requiring full logout/login in ≥95% of cases; downgrades trigger secured refresh.

## 3.E Conflict & precedence rules (clarified)

* **Mutually exclusive within a campaign:**
  + A user cannot be **Team Member/Co‑Lead** and **Campaign Support** for the **same** campaign simultaneously. Accepting one role **revokes** the other (most recent invite wins; admin warned before sending conflicting invites).
* **Owner donate rule (COI):**
  + **Only the Team Lead/Organizer** may donate to their **own** campaign (flagged).
  + Co‑Lead/Member/Support/Org Admin/Org Support **cannot** donate to that campaign.
* **Role stacking across scopes:**
  + User can be Team Member on Campaign A and Campaign Support on Campaign B; **no conflict**.
* **Organization vs Campaign scopes:**
  + **Org Support** with access to a campaign **does not** automatically become a **Team Member** on that campaign; they remain a separate role with limited permissions.

**AC**

* AC‑CON‑1: Sending a conflicting invite shows a **warning** and requires confirmation.

## 3.F Removing roles & leaving organizations

* **Campaign roles:** Lead or Co‑Lead can remove Members/Support; Co‑Lead cannot remove Lead. Lead cannot remove self without transferring ownership.
* **Organization roles:** An **Org Admin** can remove other Org Admins (must always leave at least **one** Org Admin), and Org Support.
* **Effects:** removal sets RoleBinding to **revoked\_at=now**; access ends immediately; referral links for Members are invalidated.

**AC**

* AC‑REM‑1: If removing the **last Org Admin**, the action is blocked with copy: “An organization must have at least one admin.”

## 3.G Admin override & recovery (for mismatched email or special cases)

* **Admin Console → Role Assignments**
  + Search invite; **Force‑assign** to a specific **user\_id** (even if emails differ).
  + **Reason required** + confirmation modal; writes to **AuditLog**.
  + Sends notification to both inviter and assignee.

**Use cases:** executive changeovers, legal requests, user lost email access.

**AC**

* AC‑OVR‑1: Force‑assignment requires **Super Admin** or **Org Admin with elevated approval** (secondary approver flow optional for Phase‑2).

## 3.H Security & verification steps (step‑ups)

* Accepting high‑privilege roles (Org Admin, Campaign Lead/Co‑Lead, Support with **Export CSV** permission) prompts **SMS OTP** if the user hasn’t re‑authenticated in the last **12 hours**.
* Changing payout destination (already covered) requires OTP + cooldown.
* Assigning **Export CSV** permission to someone triggers a warning: “Exports include donor contact for non‑anonymous donors. Ensure you have consent to contact.”

**AC**

* AC‑SEC‑2: Step‑up logs method and timestamp to **AuditLog**.

## 3.I Notifications (email + in‑app)

* Invite sent (to invitee)
* Invite accepted (to inviter)
* Invite expired (to inviter)
* Role changed (to affected user)
* Role removed (to affected user)
* Force‑assignment override (to inviter & assignee)

**AC**

* AC‑NOTIF‑2: All role events appear in the **Notifications log** with filter “Access & roles”.

## 3.J UI copy (ready for interface)

* **Invite email subject:** “{Org/Campaign} invited you to be **{Role}** on {Brand}”
* **Switch account modal:**
  + “This invite is for **{email}**. You’re signed in as **{current\_email}**. To accept, please switch to **{email}** or ask your admin to resend the invite.”
* **Conflicting role warning:**
  + “{email} already has **Campaign Support** on this campaign. Inviting them as **Team Member** will remove Support access. Continue?”
* **Role removed:**
  + “Your **{Role}** access to **{Campaign/Org}** has ended.”

## 3.K Acceptance criteria (summary)

* **AC‑INV‑3/4:** Invites are single‑use, **email‑bound**, 7‑day expiry; acceptance requires matching email unless Admin overrides.
* **AC‑LIVE‑1:** Role changes take effect mid‑session; sensitive downgrades force refresh.
* **AC‑CON‑1:** Conflicting invites prompt confirmation; accepting the new role revokes the conflicting one.
* **AC‑REM‑1:** Cannot remove last Org Admin.
* **AC‑SEC‑2:** Step‑up OTP for high‑privilege acceptance and sensitive permissions.
* **AC‑OVR‑1:** Admin override requires elevated privileges + reason; audited.
* **AC‑SURF‑1/2:** People directories display seat counts; all changes audited.
* **AC‑COI matrix enforced** at checkout (as already specified).

## What this means for sign up / login UX (end‑to‑end)

* **New invitee** → Registration (phone OTP + email verify auto‑confirmed from invite) → Accept role → land in the correct dashboard.
* **Existing user, logged out** → Login (prefilled invite email) → Accept role → land in dashboard.
* **Existing user, logged in with same email** → one‑click accept.
* **Existing user, logged in with different email** → Switch‑account flow (or request resend to current email).
* **Admin override** available for special cases (with audit).

# 

# Section 4 — Performance, Accessibility & UX Standards

## 4.0 Scope & goals

**Scope:** Design tokens, components, keyboard patterns, form standards, copy & error patterns, motion, theming, and **hard performance budgets** (LCP/CLS/JS/CSS).  
**Goals:** (1) Friction‑free donating, (2) WCAG 2.2 AA compliance, (3) Fast on mid‑range mobile over 4G, (4) Consistent, reusable components.

## 4.1 Design tokens (foundations)

### 4.1.1 Color tokens

* **Semantic palette (do not hardcode hex in components):**  
  --color-bg, --color-surface, --color-border,  
  --color-text, --color-text-muted,  
  --color-primary, --color-primary-hover, --color-primary-contrast,  
  --color-success, --color-warning, --color-danger, --color-info,  
  --color-focus-ring, --color-link, --color-link-visited.
* **Contrast rules:** normal text ≥ **4.5:1**, large text (≥18px regular or ≥14px bold) ≥ **3:1**; icons/non‑text UI ≥ **3:1**.
* **State tokens:** --btn-bg, --btn-bg-hover, --btn-bg-disabled, --field-bg, --field-border, --field-border-error, --field-help, --chip-bg, --chip-text.
* **Dark mode:** token set prepared; **Phase‑2** to enable (Section 10 “nice‑to‑haves”).

**AC‑TOK‑COLOR‑1:** No component ships with a hardcoded color; must consume tokens.  
**AC‑TOK‑COLOR‑2:** Primary CTAs always meet contrast vs their background.

### 4.1.2 Typography

* **Scale:** 12 / 14 / 16 / 18 / 20 / 24 / 32 / 40 / 48.
* **Line‑height:** 1.5 body; 1.25 headings.
* **Minimum body:** 16px; small helper text 14px; never below 12px.
* **Letter‑spacing:** default; avoid tight kerning on long text.

**AC‑TYPO‑1:** Public copy reads at US grade **7–9**; critical instructions ≤ grade **6**.

### 4.1.3 Spacing & layout

* **8‑pt grid**: spacing tokens 4 / 8 / 12 / 16 / 24 / 32 / 40 / 48 / 64.
* **Breakpoints:** sm 480, md 768, lg 1024, xl 1280.
* **Containers:** max content width **1200px** (campaign pages); gutters ≥ 24px desktop, 16px mobile.

### 4.1.4 Iconography

* SVG sprite or components. All meaningful icons have aria-label or paired text; purely decorative icons aria-hidden="true".

## 4.2 Interaction & keyboard patterns

### 4.2.1 Global navigation

* **Skip link:** “Skip to main content” first focusable item.
* **Focus management:** On route change, move focus to page <h1>.
* **Focus visible:** Use --color-focus-ring; 2px outline; never suppressed.

### 4.2.2 Component keyboard maps (WCAG 2.2 compliant)

* **Button:** Enter/Space activate.
* **Link:** Enter activates. Avoid div role="button".
* **Menu / Dropdown:** Enter/Space to open; Esc to close; arrow keys navigate; Home/End jump; focus trapped inside while open.
* **Modal / Dialog:** focus trap; Esc closes; return focus to invoker; labelled by visible heading.
* **Tabs:** arrow keys left/right; Home/End; Tab moves into panel.
* **Accordion:** Enter/Space toggle; arrow up/down move between headers.
* **Combobox / Autocomplete (search/typeahead):** ARIA 1.2; ArrowDown opens; Enter selects; announces results count via aria-live="polite".
* **Carousel / Gallery:** arrow keys; no autoplay; aria-roledescription="carousel"; keyboard & swipe supported; Esc closes lightbox.
* **Toast / Inline alert:** role="status" (polite) for success/info; role="alert" (assertive) for critical errors.

**AC‑KB‑1:** No keyboard traps. All interactive components pass axe‑core keyboard checks.

## 4.3 Forms & validation (global)

### 4.3.1 Structure

* Every input has a **visible label** (not placeholder).
* **Help text** uses aria-describedby; **errors** use aria-invalid="true" and an inline message.
* Numeric fields use type=number but **never rely** on spinner controls; support direct typing.

### 4.3.2 Validation patterns

* **Inline on blur** + on submit; error summary at top for long forms.
* **Phone**: E.164; format on blur: (555) 555‑5555.
* **Email**: RFC basic regex; MX not required.
* **Address**: USPS/Smarty autocomplete (10.B).
* **Currency**: whole dollars only (MVP), enforce min **$5**; sanitize to integers.

### 4.3.3 OTP flows (registration, phone change)

* 6‑digit inputs with one field per digit (auto‑advance); paste supports full code; fallback single text field if assistive tech detected.
* Countdown & resend after 60s; voice fallback per Section 18.

**AC‑FORM‑1:** Screen readers announce validation errors **once** via aria-live="assertive".  
**AC‑FORM‑2:** All required fields marked and announced (“required”).  
**AC‑FORM‑3:** Multi‑step wizards preserve values on back/forward and after soft reloads.

## 4.4 Motion & states

* Respect **prefers‑reduced‑motion** → disable parallax, smooth scroll, heavy animations; use fade/translate ≤ 150ms.
* Loading uses **skeletons** for cards/tables and **spinners** for short waits (<800ms).
* Avoid **autoplay video**; never auto‑play audio.

**AC‑MOTION‑1:** With reduced‑motion, donate progress updates use **no animation** but still announce changes.

## 4.5 Component library (baseline set)

**Buttons:** Primary/Secondary/Tertiary/Destructive; sizes (M/L); disabled state; loading state with spinner & aria-disabled="true".

**Inputs:** Text, Email, Phone, Number (whole $), Textarea, Select, Radio, Checkbox, Switch, Slider (rare), File Upload (drag‑drop + browse; keyboardable).

**Date picker:** Keyboard‑accessible; or use two selects (month/year) + day grid. Provide manual text input for accessibility.

**Table:** Sticky header, row focus, responsive collapse to cards on mobile; caption; sortable columns with aria-sort.

**Pagination:** “Prev/Next” + numbered; rel="prev/next" for SEO lists.

**Cards:** Campaign, Organizer, Team; always include semantic heading.

**Chips/Badges:** “Trending”, “Ending soon”, “AoN”, “Verified”.

**Progress bar:** Show % funded; includes text for SR (“75% funded”).

**Modals/Drawers:** Scroll lock; focus restore; close on overlay click (not for destructive confirms).

**Toasts:** stack in corner; auto‑dismiss with pause on hover; provide “View” link for important items.

**Tooltips:** Long‑press support on mobile; avoid essential content in tooltips.

**Uploader & Cropper:** Keyboardable crop handles; aspect hints (12.C).

**Accessibility kit:** Alert, Status, Live region utilities.

**AC‑COMP‑1:** Components shipped with unit + a11y tests and stories documenting keyboard support.

## 4.6 Page‑type performance budgets (mid‑range Android over 4G)

“Green” budgets are **hard**; “yellow” is degrade but acceptable during A/Bs, not for MVP.

| **Page type** | **LCP (s) ≤** | **CLS ≤** | **TBT (ms) ≤** | **JS (gz) ≤** | **CSS (gz) ≤** | **HTML ≤** |
| --- | --- | --- | --- | --- | --- | --- |
| **Home** (9,16) | 2.5 | 0.10 | 200 | 170 KB | 50 KB | 50 KB |
| **Search/Category** (16) | 2.5 | 0.10 | 200 | 180 KB | 60 KB | 50 KB |
| **Campaign page** (13) | 2.5 | 0.10 | 200 | 190 KB | 60 KB | 60 KB |
| **Checkout sheet** (14) | 1.5 | 0.05 | 100 | 120 KB | 30 KB | 35 KB |
| **Portal pages** (10) | 1.2–1.8 | 0.05 | 150 | 160 KB | 50 KB | 50 KB |
| **Admin** (20) | 1.8–2.2 | 0.10 | 200 | 220 KB | 70 KB | 60 KB |

**AC‑PERF‑1:** Each route includes **Web Vitals** reporting to analytics (FID/INP/LCP/CLS).  
**AC‑PERF‑2:** Ship **code‑split routes**; lazy‑load heavy modules (charts, editor, video).  
**AC‑PERF‑3:** Third‑party scripts **asynchronously**; avoid layout shifts; preconnect to Stripe/Twilio origins where needed (14,18).

## 4.7 Asset optimization

* **Images:** AVIF/WebP + responsive srcset; width hints; lazy‑load below fold; placeholders; decoding="async".
* **Video:** Poster images; preload="none"; do not autoplay; no inline base64 for big posters.
* **Fonts:** System stack preferred; if web fonts, use font-display: swap; subset & preload one WOFF2.
* **Caching:** CDN cache for static; immutable hashed assets; HTML no‑store for personalized pages.

**AC‑ASSET‑1:** All images require **alt**; decorative set role="presentation" or aria-hidden="true".  
**AC‑ASSET‑2:** Hero images ≤ **500 KB** mobile rendition (CMS enforces; §9).

## 4.8 Content & microcopy standards

* **Tone:** warm, helpful, plain English. No blame; give next steps.
* **Structure:** Lead with **action** → consequence → link.
* **Numbers:** currency with thousands separators; 2 decimals only on receipts/finance; whole dollars in inputs.
* **Dates:** “Oct 23, 2025” (viewer’s timezone).
* **AoN disclosure:** consistent chip + tooltip copy (13.2).

**Error pattern**

* **Title:** brief (“We couldn’t verify your code”).
* **Why:** human reason if safe (“Code expired”).
* **Fix:** one action with link/button.
* **Help:** “Need help? Contact Support.”

**Empty‑state pattern**

* Icon + one‑line explanation + primary CTA + optional link to docs.

**AC‑COPY‑1:** All critical flows have **friendly** error & empty states (Registration, Donate, Rewards, KYC, Payouts).  
**AC‑COPY‑2:** Tooltips use sentence case; avoid jargon (e.g., explain “All‑or‑Nothing”).

## 4.9 Accessibility checks & QA gates

* **Automated:** axe‑core CI on Storybook; Lighthouse CI budgets; unit tests for keyboard interactions.
* **Manual:** NVDA + VoiceOver sweeps for checkout and campaign page; keyboard‑only donate; screen reader for OTP flow.
* **Color‑blind review:** simulate deuteranopia/protanopia for state colors (success/warning/danger must remain distinct).

**AC‑A11Y‑QA‑1:** No **high** severity a11y issues; **medium** tracked; **low** scheduled.  
**AC‑A11Y‑QA‑2:** QA checklist required on each feature PR (see §4.13).

## 4.10 Internationalization & locale readiness (US‑only MVP)

* **Currency** fixed USD; formatting centralized.
* **Time** localized to viewer; avoid hard‑coded time zones in copy.
* **Text expansion ready:** avoid brittle widths; accommodate 30% expansion.

**AC‑I18N‑1:** All UI strings externalized to a messages file even if EN‑only day‑1.

## 4.11 Security & privacy UX tie‑ins

* Don’t show **why** a risk rule blocked a payment in detail; provide neutral copy + Support route (Section 5).
* Sensitive actions require **double confirm** (e.g., deletions, refunds).
* Show **cooldowns** clearly (phone change → 24h payout cooldown).

## 4.12 Print & export UX

* Receipts and payout statements have **print styles** (white background, black text, no nav).
* Exports (CSV/PDF) have column headers, units, and timezone noted.

## 4.13 Developer & QA checklists (ship gates)

**Developer pre‑merge**

* Uses tokens; no hardcoded colors
* Keyboard path covered; aria-\* labels set
* No focus loss; focus returned to invoker
* Form labels + aria-describedby wired
* Web Vitals instrumentation included
* Code‑split where >50 KB extra JS
* Images use srcset & lazy‑load
* No inline secrets; URLs behind env
* Copy reviewed (tone, grade level)

**QA pre‑release**

* Keyboard‑only flow works (donate, register, OTP, claim reward)
* Screen reader reads form labels and errors correctly
* Lighthouse: budgets met on target pages
* Mobile checks on mid‑range device
* Error/empty states present
* Motion reduced mode respected
* Third‑party scripts async/defer
* CLS checked on sticky donate/headers

## 4.14 Acceptance Criteria (summary)

* **Consistent tokens** used everywhere; contrast ratios met.
* **Keyboard & SR** patterns implemented; no traps; focus visible & restored.
* **Forms** labeled, validated with aria- attributes; OTP flows accessible.
* **Motion** reduced when requested; carousels non‑autoplay; videos not auto‑playing.
* **Performance budgets** met per page type (Web Vitals logged); route‑level code splitting.
* **Assets** optimized (AVIF/WebP, srcset, lazy); fonts swapped.
* **Copy** follows tone, error pattern, empty‑state pattern.
* **A11y QA** automated + manual gates in CI & pre‑release.
* **I18N‑ready** strings; times rendered in viewer’s timezone.
* **Print styles** for receipts; exports readable.

## 4.15 Roadmap (Phase‑2)

* Full **dark mode** theming with token parity.
* **Design tokens to code** pipeline (Figma → JSON/TS).
* **Accessible data viz** components (bar/line charts with text tables).
* **PWA** for portal (offline receipts viewer).
* **Semantic search** with accessible results highlighting.

# 

# Section 5 — Risk, Fraud & Abuse

## 5.0 Scope & objectives

**Scope:** Payment fraud prevention, account abuse, refund abuse, dispute handling, reserves/holds, deny/allow lists, messaging spam controls, and manual review.  
**Objectives:**

1. Maximize **donation conversion** while minimizing chargebacks.
2. Protect organizers, donors, and the platform.
3. Keep decisions **auditable** and **explainable**.
4. Enforce your policies (US‑only, prohibited categories, donors‑only report, COI, etc.).

**Guardrail principle:** Friction only when risk warrants it (step‑ups before hard blocks).

## 5.1 Threat model (representative)

* **Card fraud**: BIN attacks, card testing, stolen PANs, high‑velocity small donations, repeat failures.
* **Friendly fraud**: donor denies participation → chargeback; reward disputes.
* **Refund abuse**: organizers mass‑refund then leave; donors mass‑refund after rewards shipped.
* **Account takeovers (ATO)**: credential stuffing, SIM swap, session hijack.
* **Organizer fraud**: false story, misappropriation; payout to mismatched bank.
* **Money movement laundering**: many related cards to one organizer; circuitous refunds.
* **Messaging abuse**: spam, phishing, harassment.
* **Policy abuse**: prohibited content, raffle/lottery, adult, weapons.

## 5.2 Risk engine architecture

**Where it runs**

* **Account level**: on registration, login, profile/phone/email changes.
* **Checkout level**: **pre‑confirmation** of Stripe Payment Intent and at **webhook** time.
* **Payout level**: when creating payout and when Connect events arrive.
* **Messaging level**: on new DM threads/messages.

**Core components**

* **Signals collector** → **Rules engine** (deterministic first) → **Risk score** (0–100) → **Decision**:  
  **Allow**, **Allow+Monitor**, **Step‑up** (3DS, extra OTP, selfie if organizer), **Queue Review**, **Block**.
* **Audit**: persist signals, rule hits, and final decision with reason codes.
* **Configs**: admin‑editable thresholds & lists (20.I/20.P).
* **Outcomes loop**: disputes/refunds feed back into device/card/IP reputations.

## 5.3 Signals (inputs) — MVP

**Payment / device**

* Card BIN risk tier (domestic vs high‑risk foreign; pre‑paid/gift).
* AVS/CVV result; 3DS frictionless vs challenged.
* Velocity: **per card**, **per donor**, **per IP/device**, **per campaign** (windowed: 1m/1h/24h).
* IP reputation (VPN/proxy/Tor), geo vs profile state mismatch.
* Device fingerprint (hash of UA + IP + client hints; privacy‑safe).
* Decline codes (do\_not\_honor, stolen\_card), repeated declines.

**Account / behavior**

* Account age, email domain age, phone carrier type, verified phone/email.
* Prior disputes/refunds linked to user/card/device/IP.
* COI/affiliation (team member donating to own campaign).
* Unusual amount vs campaign average; high custom amount outside presets.

**Organizer / campaign**

* KYC state (ID/SSN/EIN), bank name mismatch flag (11.5).
* Story/Media completeness; prior suspensions; reported status.
* Donation mix anomalies (high % from same BIN or IP range).

**Messaging**

* New‑thread velocity, URL count, profanity/harassment dictionary matches (light filter).

**Privacy:** Store **partial BIN (6–8), last4, hashed device id**, never full PAN (Stripe holds it).

## 5.4 Rules & thresholds (defaults; admin‑tunable)

### 5.4.1 Velocity throttles (real‑time)

* **Global (donations):** **max 3 per minute, 10 per hour** per account/IP (you approved in §14.I.34).
* **Per card:** max **2 attempts** per minute; **5** per hour; **10** per day.
* **Per donor → same campaign:** max **$5,000/day** (hard stop) & **$10,000/week** (step‑up).
* **Per donor → all campaigns:** **$10,000/day** (step‑up), **$25,000/week** (manual review).
* **Per IP** (unauthenticated endpoints): if exceeded, show CAPTCHA then block until cooldown.

### 5.4.2 Amount & method rules

* **Single donation ≥ $5,000** → force **3DS challenge** (if card supports) and email confirmation after payment.
* **Single donation ≥ $10,000** → **manual review** (funds accepted but **held** against payout).
* **Gift/prepaid** cards: allow ≤ **$500** per day; above triggers step‑up.
* **Non‑US cards:** allowed (USD), but if BIN risk high + IP mismatch → step‑up or block.

### 5.4.3 Location & identity

* IP state differs from profile state by > 2 states **and** account age < 1 day → step‑up (extra OTP) or 3DS.
* Unverified phone/email → require verification **before** first donation ≥ $500.

### 5.4.4 Organizer & COI

* **Team Co‑Lead/Member/Support** donating to own campaign → **block** (policy; §13.3).
* Organizer self‑donation allowed but **flagged**; counts toward velocity & risk monitoring; show COI banner.
* Organizer with **Compliance Hold** → donations allowed (to avoid donor friction) but **payouts locked**.

### 5.4.5 Content & policy

* Campaign flagged “Under review” → donations **paused**.
* Prohibited categories (weapons/adult/raffles) → auto block at creation (Section 0.F.4) and remove from discovery.

## 5.5 Decisions & step‑ups

* **ALLOW**: proceed to confirmation; log risk score.
* **ALLOW + MONITOR**: tag donation for post‑monitor; include in anomaly dashboards.
* **STEP‑UP**:
  + **3DS** (cardholder auth).
  + **Extra OTP** to donor’s phone (if already verified).
  + **Organizer selfie/liveness** (for payout or publish; §11.7).
* **QUEUE REVIEW**: accept funds, **hold** for payout; ticket to **Risk Review** queue.
* **BLOCK**: clear UI message (“We couldn’t process this donation. Try a different method or contact Support.”); record reason.

**SLAs**

* Queue Review targets: **< 24 hours** (business) for large donations; **< 2 hours** for obvious card testing bursts (auto‑decline).

## 5.6 Manual review workflow (Admin → Risk)

**Queue views**: Card testing, High‑amount, Velocity abuse, Device/IP clusters, Organizer mis‑match.  
**Evidence pane** (read‑only): donation data, device/IP, AVS/CVV, 3DS outcome, account age, KYC state, prior history, related donations, messaging reports.  
**Actions**: **Approve**, **Decline**, **Request more info** (donor/organizer), **Place reserve** (pct/time), **Suspend campaign**, **Ban account**, **Add to lists**.  
**Audit**: every action with reason code; dual‑approval for declines ≥ $5,000.

## 5.7 Lists & reputation

* **Deny list**: cards (token), emails, phones, device IDs, IPs/CIDR, BINs, domains.
* **Allow list**: VIP donors (corporate philanthropy), trusted BINs.
* **Gray list**: temporary cooling (e.g., 24–72h) for suspicious bursts.

**Admin UX**: bulk import, expiry, notes, hit‑rate stats; conflicts resolved by **Allow > Deny** with warning.

## 5.8 Reserves & payout holds

* **Standard hold**: You set 3–5 **business** days after campaign end (§15.D.22).
* **Dynamic reserve** (by risk): **0–20%** of net for **30–60 days** when: dispute rate last 30d ≥ 0.5%, rapid velocity spikes, organizer KYC friction, returned payouts.
* **Per‑campaign** reserve overrides via Risk/Finance with reason and end‑date.

**AC (reserves)**

* Reserve balances shown in Wallet (10.D), with release schedule.
* All holds/reserves block only **payouts**, not donation acceptance.

## 5.9 Chargebacks (disputes) & representment (Stripe)

**Intake**: charge.dispute.created (Section 7.4).  
**Auto‑assembled evidence pack** (download/edit before submit):

* Receipt & terms (ToS, Refund policy), donor IP/device, AVS/CVV & 3DS outcome, donor account age & history, reward status (Pending/Processed), messages between donor & organizer (if relevant), organizer verification status.  
  **Deadlines**: Stripe due date → Admin SLA (reminders at T‑7/T‑3/T‑1 days).  
  **Outcomes**: won/lost/closed mirrored; dashboards track chargeback rate and loss.

**Policy link**: Donor protection for **proven fraud** (Section 0.F.32) → full refund.

## 5.10 ATO (account takeover) protections

* **Login anomaly detection**: new device + new geo → email alert; optional TOTP prompt.
* **Password change & phone change**: step‑up with TOTP/SMS; **24h payout cooldown** (§10.O.38).
* **Session management**: show devices; “Sign out all others” (10.C.7).
* **SIM‑swap check** (Phase‑2 add‑on; §11.13.C): on high‑value events.

## 5.11 Messaging (DM) abuse controls (tie to 10.S)

* **Thread limits**: **5 new conversations/day**, **30 messages/hour** (per user); Admin‑tunable.
* **Content filter**: profanity/harassment dictionary; link throttling (≥2 links → warning/slow mode).
* **Report & block**: instant; block prevents new threads; reports create **Moderation case**.
* **Donors‑only** option for organizers (default **Anyone**, can switch to **Donors‑only**).

## 5.12 Admin Console (20.B & 20.D) tie‑ins

* **Risk dashboard**: chargeback rate, refund rate, dispute pipeline, reserves, top risky BINs/IPs, velocity alerts.
* **Rule editor**: sliders for thresholds (velocity/amount), toggles for step‑ups, BIN tiers, IP ranges, allow/deny lists.
* **Case management**: review queues, evidence upload, decision templates, dual‑approval for high‑value declines/reserves.
* **Simulation**: test rule set on last 30 days of traffic before apply (shadow mode).
* **Audit**: all rule changes logged (who/what/when), with rollback.

## 5.13 Data model (additions to §8)

**risk.rule\_set**

* id, name, version, active bool, params jsonb (thresholds), created\_by, created\_at.

**risk.signal\_log**

* id, donation\_id NULL, user\_id NULL, campaign\_id NULL, context ('checkout'|'login'|'payout'|'message'), signals jsonb, risk\_score int, rule\_hits text[], decision enum('allow','monitor','step\_up','review','block'), reason\_code, created\_at.

**risk.case**

* id, type ('high\_amount','velocity','organizer','messaging','other'), status ('open','approved','declined','more\_info','closed'), priority, assignee\_user\_id, subject\_ref (donation\_id|user\_id|campaign\_id), notes, history jsonb, opened\_at, closed\_at.

**risk.list\_item**

* id, kind ('allow','deny','gray'), target\_type ('bin','card\_token','email','phone','device','ip','cidr','domain'), target\_value, expires\_at, notes, created\_by.

**finance.reserve**

* id, campaign\_id, wallet\_id, percent int, start\_at, release\_at, reason\_code, created\_by, status ('active','released','canceled').

## 5.14 APIs & webhooks bindings (to §7)

* **Before PI confirmation** call Risk service → decision & metadata; if **block**, do not create/confirm PI.
* **On webhook** (payment\_intent.succeeded|payment\_failed|charge.refunded|charge.dispute.\*) update **risk.signal\_log** (outcomes) and reputation.
* **Admin** endpoints for lists, rules, decisions with step‑up privileges and audit.

## 5.15 Acceptance Criteria (summary)

* Velocity limits enforced with clear, friendly UX; CAPTCHA where applicable.
* High‑amount donations trigger appropriate **step‑ups** and/or **manual review** with payout holds.
* COI rule blocks non‑owner team members from donating to their own campaign; organizer self‑donations flagged.
* Non‑US & prepaid cards permitted but scrutinized; thresholds adjustable.
* Deny/allow/gray lists available with expiry and audit; allow overrides deny with warning.
* Disputes auto‑assemble evidence; reminders fire; outcomes update analytics.
* Reserves visible in Wallet and governed by reasoned rules; release schedule respected.
* ATO protections in place; payout cooldown after sensitive changes; device/session list works.
* DM abuse controls active; rate limits; report/block; moderation case creation.
* All decisions **auditable**: signals, rules hit, decision, actor, timestamp.
* Monitoring: dashboards for risk KPIs; alerts for BIN attacks, webhook failures, dispute spikes (tie to §21.5).

## 5.16 Microcopy (ready to ship)

* **Velocity block (donor):** “You’ve reached the limit for donations in a short period. Please try again later or contact Support.”
* **High amount step‑up:** “For your security, we’ll confirm a few details before processing this larger donation.”
* **COI block:** “You’re part of this campaign’s team, so you can’t donate here. Only the campaign owner can donate.”
* **Paused under review:** “This campaign is temporarily unavailable while we review a report.”
* **Reserve notice (organizer):** “A temporary reserve of **{percent}%** applies until **{date}** to protect against disputes.”
* **Dispute reminder:** “Evidence for dispute **{id}** is due on **{date}**. Add documents now.”

## 5.17 Roadmap (Phase‑2)

* **IP reputation provider** (e.g., Cloudflare Security Events or IPQS) integration.
* **ML risk scoring** (logistic regression/GBM) trained on historical outcomes.
* **Behavioral biometrics** (keystroke/mouse heuristics) with strong privacy guardrails.
* **Graph analytics** for ring detection (shared devices/cards across multiple accounts).
* **Adaptive step‑ups**: personalized based on donor history.
* **Content ML** for campaign/story anomalies and image OCR (policy screening).
* **Friendly fraud pledges** (organizers opt‑in to evidence standards for higher trust score).

# 

# Section 6 — Privacy, Data Retention & Legal

**6.0 Scope & goals**

**Scope:** What data we collect, why, where it lives, how long we keep it; consent & cookies; user privacy controls; DSAR workflows (access/export/correction/deletion/opt‑out); “Do Not Sell/Share”; marketing & SMS consent; children’s policy; sensitive data constraints; admin governance; auditability.  
**Goals:** (1) Protect donors & organizers, (2) Minimize risk and exposure, (3) Comply with U.S. privacy laws baseline + “GDPR‑ready” posture, (4) Keep records and flows **auditable** and **automatable**.

**6.1 Roles & responsibilities**

* **We** are the **Data Controller** of user and campaign data.
* **Vendors** (Stripe, SendGrid, Twilio, Zendesk, Smarty, cloud) are **Processors/Sub‑processors**.
* **Stripe** holds raw PAN/SSN/ID images (we store **tokens/statuses only**, per §7 & §11).
* **Admins** access PII on a least‑privilege basis (SSO + 2FA + step‑up per §20.A).

**AC‑ROLE‑1:** Sub‑processor registry exists in Admin (owner, data categories, country, DPA status).  
**AC‑ROLE‑2:** All high‑risk Admin actions are logged to admin.audit\_log.

**6.2 Data inventory & classification**

**Classes (impact tiers):**

* **P0 Highly sensitive:** payment tokens, government ID tokens/status, SSN last‑4 token/status, bank account tokens, security recovery codes. *(Stored as tokens/status with vendors; never raw)*
* **P1 Sensitive/PII:** name, email, phone (E.164), address, DOB.
* **P2 Account/usage:** username, device & IP metadata (coarse), session ids, preferences, notifications, consent logs.
* **P3 Public content:** campaign story/media, organizer name/location (city/state), public stats (toggleable), public comments (Phase‑2).

**AC‑INV‑1:** Every table/field mapped to a class; access paths documented (see §8 schema + Appendix 6.A data map).  
**AC‑INV‑2:** P0/P1 encrypted at rest, P0 redacted from logs.

**6.3 Legal basis & consent model (U.S. baseline, GDPR‑ready)**

* **Contract necessity:** account, campaign creation, donations, payouts, security.
* **Legitimate interests:** fraud prevention, safety, service analytics (first‑party).
* **Consent:** marketing email, SMS, cookies beyond strictly necessary, and any optional data sharing.
* **A2P/TCPA:** explicit opt‑in for SMS; STOP/HELP must work (see §18 & §7.7).

**AC‑CONSENT‑1:** Consent is **granular per topic/channel**, stored with timestamp, IP, user agent, and policy/template version.  
**AC‑CONSENT‑2:** Withdraw consent from **Manage Preferences** applies within 24h (marketing) and instantly for SMS.

**6.4 Cookies, storage & tracking**

**Categories**

1. **Strictly necessary** (session, CSRF, load balancer).
2. **Functional** (remembered preferences—language/dark mode Phase‑2).
3. **Analytics** (first‑party + optional GA/Posthog; no PII).
4. **Marketing** (only if/when used; default **OFF**).

**Controls**

* **Consent banner (US baseline):** show on first visit; allow “Accept all”, “Reject non‑essential”, “Customize”.
* **Global Privacy Control (GPC):** honored as a **Do Not Sell/Share** signal.
* **Geotargeting:** US‑only service, but if non‑US browsers visit, still show banner and default to non‑essential=OFF.

**Storage rules**

* No PAN/SSN/ID in cookies/localStorage—ever.
* UTMs stored 30 days (first‑party cookie) for conversion/reports; purge on request.

**AC‑COOKIE‑1:** CMP (Consent Manager) writes a signed privacy.cookie\_consent record with version + choices.  
**AC‑COOKIE‑2:** “Do Not Sell/Share” control present in footer; persists to preference store and suppresses marketing/ads (if any).

**6.5 User privacy controls (portal)**

**Manage Privacy (Profile → Settings)**

* Download my data (export)
* Delete my account (request)
* Anonymize public donor display (toggle; subject to policy)
* Cookie preferences
* Marketing email opt‑in/out
* SMS opt‑in/out (A2P)
* **Do Not Sell/Share** (CPRA definition)
* Public profile stats visibility toggles (from §10.T.3)

**AC‑CTRL‑1:** Changes write to consent log, reflect immediately in product (except exports/deletion which are workflows).  
**AC‑CTRL‑2:** Security step‑up (password + 2FA) required for deletion requests and data exports.

**6.6 DSAR workflows (Access, Export, Correction, Deletion/Anonymization, Appeal)**

**6.6.1 Access/Export (JSON + CSV + ZIP)**

* Content: profile, emails/phones, addresses, donations (own), rewards, messages (own threads), preferences, consents.
* Excludes: other users’ PII and any secrets.
* Delivery: secure link; expires in 7 days.

**6.6.2 Correction**

* Allow user to correct PII (name, address, phone/email via verification flows); legal name change requires re‑verification (§11.6).

**6.6.3 Deletion vs Anonymization (ledger‑safe)**

* If **no donations** and **no payouts**: hard delete account + portal content (keep minimal legal logs).
* If **donations/payouts exist**: retain financial records; **anonymize public display** (replace name with “Removed User”), keep internal IDs for reconciliation.
* Delete messages & media authored by user unless retained for legal/dispute reasons.

**6.6.4 Opt‑out of sale/sharing**

* Set suppression across marketing/ads; do not load marketing pixels; do not share for cross‑context behavioral ads.

**6.6.5 Appeals (where required)**

* Simple appeal form; 45‑day SLA; results emailed; record in Admin.

**SLA & Audit**

* Acknowledge **within 10 days**; complete **within 45 days** (export/delete).
* All steps logged in privacy.dsar.

**AC‑DSAR‑1:** DSAR pipeline implemented (portal submit → Admin queue → automated exports → secure delivery).  
**AC‑DSAR‑2:** Deletion respects **ledger integrity**: donations remain but display anonymized; receipts still valid.

**6.7 Data retention & purge schedule (authoritative)**

Periods are **minimum** unless legal hold requires longer. Purge jobs run nightly; metrics visible in Admin.

| **Data category** | **System** | **Retention** | **Notes** |
| --- | --- | --- | --- |
| Donations & refunds (financial ledger) | DB (§8 donation/finance) | **7 years** | Accounting/audit. |
| Payouts & statements | DB/Export | **7 years** | Accounting/audit. |
| KYC/KYB statuses & tokens | DB (§11) | **5 years** | Don’t store raw docs. |
| ID/selfie artifacts | **Vendor only** | Vendor policy | We store **status** only. |
| Messages (DM) | DB (§10.S) | **24 months** | Unless case/legal hold. |
| Notifications delivery attempts | DB (§18) | **12 months** | For deliverability investigations. |
| Security logs, auth events | DB | **24 months** | Fraud/ATO investigations. |
| Analytics events | DB (§8.L) | **18 months** | Partitioned; no PII. |
| Moderation cases/reports | DB (§20.B) | **24 months** after close |  |
| CMS versions | DB (§9) | **24 months** | Legal pages retained indefinitely with effective dates. |
| Backups (DB PITR) | Storage | **30 days** | Encrypted, immutable bucket. |
| Uploaded assets (campaign media) | S3 | Until user deletes campaign or legal hold lifted | Quarantine & AV policy applies. |

**AC‑RET‑1:** Purge job emits report (deleted counts) and appends to admin.audit\_log.  
**AC‑RET‑2:** Backups aging out do not violate legal holds (tagged snapshots).

**6.8 Sensitive data & prohibited content**

* We are **not** a HIPAA covered entity. **Do not** submit protected health information (PHI) in stories, images, or messages.
* Prohibit: full SSNs, bank numbers in free text, medical records, explicit adult content, weapons/raffles, hate/harassment (per Community Guidelines).
* Medical campaigns: allow narratives but **redact** PHI in public text.
* Optional (Phase‑2): PII/PHI **content scanner** on uploads (server‑side) with soft warnings or blocks.

**AC‑SENSE‑1:** Upload forms warn users not to include PHI/financial numbers.  
**AC‑SENSE‑2:** Moderation can remove media/sections and require edits (§20.B.10).

**6.9 Children’s privacy**

* Service is **18+ only** (validated via ID). No child accounts; no knowingly collected children’s data.
* Profiles and campaigns about minors must be created by **adults**; content still must avoid PHI.

**AC‑COPPA‑1:** Registration enforces 18+; under‑age attempt shows policy copy and blocks.

**6.10 Public transparency & legal documents (published via CMS §9)**

**Documents (initial set)**

* **Privacy Policy** (data map, rights, retention, cookies, GPC, DSR instructions)
* **Terms of Use** (contract, prohibited uses, campaign rules, fees, AoN/KWR, dispute venue)
* **Community Guidelines** (content, behavior, report process)
* **Refunds Policy** (organizer/admin controlled; AoN auto‑refunds)
* **Security Overview** (controls; how to report a vulnerability)
* **Accessibility Statement**
* **Data Processing Addendum** (for orgs that require it)
* **Sub‑processor List** (automatically generated from Admin registry)

**Governance**

* Legal pages require **two‑person approval** to publish (per §9.9).
* **Effective date** and prior versions linked.
* Significant changes: notify users via email/in‑app; collect **re‑consent** where needed.

**AC‑DOC‑1:** All public legal pages have anchors + ToC; are indexable; and link to the **DSAR request** page.  
**AC‑DOC‑2:** Sub‑processor list is current; changes are timestamped and optionally notify users.

**6.11 Marketing & communications consent**

* **Email:** Transactional always on; marketing **opt‑in** only. CAN‑SPAM compliant footers, one‑click unsubscribe on marketing.
* **SMS:** Transactional (OTP, payout alerts) permissible; marketing **off** (day‑1). Respect STOP/UNSTOP/HELP.
* **In‑app:** always on for service events; users can mute threads (DM) or switch to digests for some topics.

**AC‑COMM‑1:** Preferences UI (10.K) writes to notif.user\_preference and privacy.consent\_log.  
**AC‑COMM‑2:** Suppression lists honored across all senders (SendGrid/Twilio).

**6.12 Security, minimization & privacy‑by‑design**

* **Minimize**: collect only what’s needed to provide donations & payouts.
* **Encrypt** P0/P1 at rest; TLS in transit.
* **Access**: least privilege; quarterly reviews; joiner/mover/leaver process within 24h (§21.10).
* **Logs**: no P0 data; scrub query params; rotate keys (§7.2).
* **Design gates**: PR template includes privacy checklist (data collected, purpose, retention, user control).

**AC‑PBD‑1:** New features require a **Privacy Impact Note** (stored in Admin) if touching P0/P1.

**6.13 Admin console surfaces (tie‑ins)**

* **Privacy Center (Admin → Compliance):** DSAR queue & status; retention purge dashboard; sub‑processor registry; cookie/CMP configuration; legal doc versioning; GPC toggle; “Do Not Sell/Share” routing rules; marketing suppression explorer.
* **Actions:** approve/deny/appeal DSAR; export regenerate; delete/anonymize; add/remove sub‑processor; publish legal pages; edit cookie banner copy; run purge preview.
* **Audit:** every action recorded (actor, reason, timestamp, diff).

**AC‑ADMIN‑1:** DSAR and Purge jobs show metrics; failures page with retry.  
**AC‑ADMIN‑2:** Cookie banner variations (A/B) tracked & versioned (Admin 20.H + 20.Q).

**6.14 Data model (additions to §8)**

privacy.consent\_log

- id, user\_id (nullable for anonymous cookie logs), context ('account','cookie','marketing','sms','do\_not\_sell\_share'),

version, choice\_jsonb, ip, ua, country, created\_at

privacy.cookie\_consent

- id, visitor\_id (anon cookie id), user\_id nullable, version, strictly\_necessary bool, functional bool, analytics bool, marketing bool, gpc\_detected bool, created\_at

privacy.marketing\_opt\_in

- user\_id, channel ('email','sms'), opted\_in bool, source ('portal','checkout','import'), version, timestamp

privacy.subprocessor

- id, name, purpose, data\_categories text[], location\_country, dpa\_on\_file bool, last\_reviewed\_at, status ('active','retired')

privacy.rota\_entry (Records of Processing Activities - lightweight)

- id, system ('donations','wallet','kyc','notifications','cms','analytics', ...), data\_categories text[], purpose, retention, legal\_basis, recipients text[], safeguards text, last\_updated\_at

*(Other referenced tables already exist: privacy.dsar, notif.user\_preference, notif.suppression, admin.audit\_log.)*

**6.15 Acceptance Criteria (summary)**

* **Consent:** granular, logged with version & evidence; withdrawals honored.
* **Cookies:** CMP with customize; GPC honored; Do Not Sell/Share control persists & routes.
* **DSAR:** end‑to‑end automation—identity verification, export, deletion/anonymization, appeal; SLA clock tracked.
* **Retention:** nightly purge jobs; reports & audits; backups lifecycle enforced.
* **Sensitive data:** P0 held by vendors only; PHI warnings present; scanners optional.
* **Children:** 18+ enforced; under‑age blocked.
* **Legal pages:** versioned, two‑person approval, effective dates, and public transparency.
* **Marketing/SMS:** opt‑in only; STOP/HELP honored; suppression unified.
* **Privacy‑by‑design:** PR checklist required for P0/P1 features; Admin register kept up‑to‑date.
* **Audits:** every privacy action recorded; reports exportable to CSV/PDF.

**6.16 Microcopy (ready to ship)**

* **Cookie banner (default):**  
  “We use cookies to make this site work and to improve your experience. You can accept all cookies, reject non‑essential cookies, or customize your choices.”  
  Buttons: **Accept all** · **Reject non‑essential** · **Customize**
* **Do Not Sell/Share:**  
  “If you live in certain U.S. states, you may opt out of ‘sale’ or ‘sharing’ of your personal information. We do not sell personal information. If you opt out, we will also stop sharing data for cross‑context advertising.”
* **Export confirmation:**  
  “We’re preparing your data export. You’ll receive a secure download link within 24 hours.”
* **Deletion request submitted:**  
  “We’ve received your request to delete your account. Financial records may be retained as required by law; your public name will be anonymized where applicable.”
* **PHI warning (campaign editor):**  
  “Please don’t include medical records or protected health information (PHI). Share only what you’re comfortable making public.”
* **Under‑age block:**  
  “You must be 18 or older to use this service.”

**6.17 Roadmap (Phase‑2)**

* **Regional policy variants** (auto‑surface state‑specific rights copy).
* **Cookie‑less analytics mode** with SSR beacons.
* **Automated PII redaction** for images (OCR) and text (NLP) on uploads.
* **Enterprise DPA self‑service** (download + e‑sign).
* **Privacy training** module tracking in Admin for staff.

# 

# Section 7 — External APIs & Webhooks

**7.0 Scope & goals**

**Scope:** Payments, Identity/KYB, Payouts, Email/SMS/Voice, Address & IRS checks, Helpdesk/KB, Media embeds, Storage/CDN, CAPTCHA, Analytics (optional), plus a **single webhook ingestion pipeline** with verification, dedupe, and replay.

**Goals:**

* Keep **raw PII off our servers** where possible (Stripe‑hosted).
* Webhooks are **durable**, **idempotent**, and **observable**.
* Integrations are **swap‑able** behind a provider abstraction.

**7.1 Providers & roles (defaults)**

| **Domain** | **Provider (Default)** | **Purpose** | **Notes** |
| --- | --- | --- | --- |
| Payments (donations) | **Stripe Payments** (Payment Intents + Elements/Payment Request) | Card, Apple Pay, Google Pay, Link; 3DS/Radar | On‑site checkout (Section 14) |
| Identity (ID/selfie) | **Stripe Identity** | DL/State ID + selfie step‑ups | Section 11 |
| KYB + Payouts | **Stripe Connect (Express)** | SSN last‑4 / EIN; US bank; returned payouts | Section 11 & 15 |
| Email | **SendGrid** (primary) → **Mailgun** (failover) | Transactional + limited marketing | Section 18 |
| SMS/Voice | **Twilio** (A2P 10DLC) + **Verify** for OTP | SMS + TTS fallback | Section 18 & registration OTP |
| Address | **Smarty** (USPS‑powered) | Autocomplete/validation | Section 10 |
| Nonprofit check | **IRS BMF/Pub 78** (via aggregator) | Verified Nonprofit badge | Section 11.13 |
| Helpdesk/KB | **Zendesk** (or Intercom) | Tickets, KB, macros | Sections 9 & 20 |
| Media embeds | **YouTube/Vimeo oEmbed** | Campaign videos | Section 12.C |
| Storage/CDN | **Amazon S3 + CloudFront** | User uploads; signed URLs; AV scan | Section 12.C; 9.3 |
| CAPTCHA | **hCaptcha** (or reCAPTCHA v3) | Bot & abuse protection | Registration, contact forms |
| Analytics (optional) | **GA4 / Posthog** (read‑only) | Top‑level web analytics | Internal analytics remain first‑party (20.T) |

**Environments:** Separate keys & endpoints for **Sandbox/Staging/Production**; strong visual environment banners in Admin (20.A.7).

**7.2 Secrets, keys & configuration**

* **Secrets store:** Vault/KMS; apps read via env vars rotated by CI/CD.
* **Rotation:** 90‑day rotation for SendGrid/Twilio; Stripe per policy; revoke immediately on suspected leak.
* **Allow‑lists:** Webhook IP ranges pinned where provider supports (Twilio) + signature verification (all).
* **Test data:** Dedicated test accounts (Stripe test keys, Twilio test credentials) in staging.

**7.3 Payments (donations) — Stripe Payment Intents**

**Flow (Section 14‑aligned)**

1. Server creates **PaymentIntent** with amount = donation\_cents (+ cover\_fees if ON) + tip\_cents, currency=USD.
2. **Automatic payment methods ON**; enable card, Apple/Google Pay, Link.
3. Client confirms PI with Elements/PaymentRequest; handle **3DS** if required.
4. On payment\_intent.succeeded → create donation.donation row; compute fee and net (either from Stripe fee breakdown via Balance Txn webhook or internal calc if cover‑fees).
5. On payment\_intent.payment\_failed → surface error; allow single **auto‑retry** (14.H.31).
6. For **AoN**: charge **now**; on not‑funded at deadline → trigger **refund** (API flow below).

**Metadata on PI/Charge**

* campaign\_id, donor\_user\_id, funding\_model\_snapshot, referral\_member\_id (nullable), utm (json), hide\_name, anonymous, cover\_fees, tip\_cents.

**Fees & amounts**

* **Tip** belongs to platform (revenue); **cover fees** increases gross so **net\_to\_campaign** ≈ donor’s intended donation amount.
* Persist Stripe’s **fee components** when balance transaction arrives.

**Idempotency**

* Client supplies idempotency\_key = hash(user\_id, campaign\_id, amount\_cents, created\_at\_floor) on “Start donation”; server reuses when creating PI.

**Acceptance Criteria (AC‑PAY)**

* AC‑PAY‑1: 3DS handled; donor returned to confirmation with preserved state.
* AC‑PAY‑2: All succeeded charges create **exactly one** donation row.
* AC‑PAY‑3: Refunds (commanded later) reconcile to Stripe Refunds webhooks and update donation status.

**7.4 Refunds & disputes — Stripe**

**Refunds**

* Initiated by Organizer/Admin (20.E.23)—no auto‑approval.
* API: stripe.refunds.create({ payment\_intent, amount }).
* Webhook: charge.refunded (or refund.updated) → update finance.refund and donation status.

**AoN auto‑refunds**

* On deadline if not funded: iterate succeeded donations, create refund(s); batch & rate‑limit; mark aon\_auto\_refunded.

**Disputes**

* Webhooks: charge.dispute.created|updated|closed.
* Store case in donation.dispute; attach **evidence kit** (receipt URL, IP/device, reward status) before due date.

**AC‑REF**

* AC‑REF‑1: Partial refunds supported; summed refund amounts ≤ original charge.
* AC‑REF‑2: Refund email receipt sent to donor (Section 18).
* AC‑REF‑3: Dispute deadlines tracked with reminders.

**7.5 Identity (Stripe Identity) — ID + selfie**

**Create verification session** → redirect to Stripe‑hosted capture.  
**Webhooks:**

* identity.verification\_session.verified → kyc.kyc\_profile.id\_status='verified' (+ age\_verified=true).
* identity.verification\_session.requires\_input or …failed → increment attempt, show retry UI; after 3 fails, open **Compliance** case.

**Selfie step‑ups (11.7)** triggered by risk engine → same session type with type=document\_and\_selfie.

**AC‑ID**

* AC‑ID‑1: We **never store** DL images or SSN—only tokens/status.
* AC‑ID‑2: Attempt limits & cooldowns enforced and visible in UI.

**7.6 KYB + Payouts (Stripe Connect Express)**

**Onboarding**

* Generate **Account Link** (Express); organizer completes SSN/EIN + bank.
* Store connect\_account\_id (privacy vault or PayoutEligibility).
* **Name mismatch** → set **Compliance Hold** and request docs.

**Payouts**

* Payout timing “**on campaign end**” (Section 15): compute eligibility (net succeeded − prior payouts).
* Initiate **Transfers** or Payouts as appropriate to connected account.

**Webhooks:**

* account.updated (requirements changes), payout.paid|failed|canceled|returned, capability.updated.
* Returned payout → set status, notify organizer (SMS + email), **resubmit** after bank update (20.D.20).

**AC‑CONNECT**

* AC‑CON‑1: Returned payouts create Finance case; resubmit preserves traceability.
* AC‑CON‑2: Dual‑approval enforced for ≥$50k or recent dest change.

**7.7 SMS/Voice (Twilio)**

**OTP (registration & phone change)**

* Use **Twilio Verify**: start verification (SMS), check code; fallback **TTS voice** if SMS undelivered in 2 min.

**Transactional SMS**

* Payout returned, payment retry needed, refund reminders (Section 18).
* Inbound **STOP/HELP/UNSTOP** handled via Twilio webhook → update **Suppression** and **UserPreference**.

**Voice fallback**

* For **OTP** and **payout returned**: TTS call with short script (18.5).

**Webhooks:**

* /webhooks/twilio/inbound-sms (STOP/HELP), /webhooks/twilio/status (DLR), /webhooks/twilio/voice-status.
* Verify Twilio signature; log DLR statuses.

**AC‑SMS**

* AC‑SMS‑1: STOP immediately suppresses further SMS except mandatory HELP/STOP confirms.
* AC‑SMS‑2: Voice fallback only on configured events; logged and visible in DeliveryAttempts.

**7.8 Email (SendGrid → Mailgun failover)**

**Sending**

* Transactional only (+ minimal marketing opt‑in).
* **SPF/DKIM/DMARC** enforced; dedicated IP warmed.
* Template keys managed in Admin 20.H (versioning & test send).

**Webhooks:**

* SendGrid: delivered, open/click, bounce, spam complaint;
* Failover rule: if delivery rate < threshold or provider outage → switch to **Mailgun** automatically.

**AC‑MAIL**

* AC‑MAIL‑1: Bounces/complaints add to **SuppressionList** and show in user preferences with self‑service re‑enable.
* AC‑MAIL‑2: All messages have List-Unsubscribe where applicable and a **Manage Preferences** link.

**7.9 Address verification (Smarty/USPS)**

**Autocomplete + verify** at point of entry (Profile, Reward claim).  
Return standardized US address (Suite/PO Box allowed) + DPV code, county, ZIP+4 when available.

**AC‑ADDR**

* AC‑ADDR‑1: We store both **user input** and **standardized form**; shipping uses standardized unless user overrides (with warning).
* AC‑ADDR‑2: Verification failures do not block (warn + allow).

**7.10 IRS nonprofit check (Pub 78 / BMF via aggregator)**

**Match logic**

* On EIN verification success, attempt name + EIN match to IRS data.
* If match → set kyb\_profile.nonprofit\_status='verified' → show **Verified Nonprofit** badge.
* Recheck monthly (scheduled job).

**AC‑IRS**

* AC‑IRS‑1: Clearly show “Unable to confirm nonprofit status” when mismatch (non‑blocking).
* AC‑IRS‑2: Store source dataset version/date.

**7.11 Helpdesk & Knowledge Base (Zendesk)**

**Tickets**

* Create via API (from Contact form) with metadata (user\_id, URL, category).
* Webhooks → /webhooks/zendesk/ticket-updated to sync status for portal ticket list.

**KB**

* Sync titles/paths; render via CMS (9.8).

**AC‑ZEND**

* AC‑ZEND‑1: SLA timers in Admin (20.G) reflect Zendesk updates within minutes.

**7.12 Media embeds (YouTube/Vimeo oEmbed)**

* Accept URLs; call **oEmbed** for title/thumbnail.
* Sanitize embeds; **no autoplay**, rel="noopener".

**AC‑EMBED**

* AC‑EMBED‑1: If video removed/private, show graceful fallback (“Video unavailable”).

**7.13 Storage/CDN & malware scanning (S3 + CloudFront)**

**Uploads**

* Client → signed S3 URL (scoped); on complete, enqueue **AV scan** (ClamAV or Lambda‑based).
* On **malware detected** → quarantine + notify moderator; block publish.

**Serving**

* CloudFront with aggressive caching, image resizing service for responsive renditions.

**AC‑CDN**

* AC‑CDN‑1: Only **scanned‑clean** assets exposed to public URLs.
* AC‑CDN‑2: Signed URLs expire ≤ 15 minutes for private assets.

**7.14 CAPTCHA (hCaptcha / reCAPTCHA v3)**

Apply to: **Registration**, **Login abuse threshold**, **Contact form**, **Report campaign** (optional), **DM new thread** (first message).  
Score threshold configurable in Admin (20.I); challenge fallback when suspicious.

**AC‑BOT**

* AC‑BOT‑1: CAPTCHA failures return friendly error; retry allowed.

**7.15 Optional analytics (GA4/Posthog)**

* Pageview & basic conversion; **no PII**.
* Respect DNT/consent; server‑side events remain first‑party in analytics.event.

**7.16 Webhook ingestion pipeline (all providers)**

**Endpoints**

* POST /webhooks/stripe (Payments, Identity, Connect)
* POST /webhooks/twilio/\* (inbound, DLR, voice)
* POST /webhooks/sendgrid (events)
* POST /webhooks/mailgun (events)
* POST /webhooks/zendesk (tickets)
* (Optional) /webhooks/irs-agg if aggregator supports push; else we **poll**.

**Security**

* Verify **signature headers** per provider (Stripe Stripe-Signature, Twilio X-Twilio-Signature, SG X-Twilio-Email-Event-Webhook-Signature/Timestamp, MG signature).
* Reject >5 minutes **clock skew**.
* **Rate limit** per endpoint; **IP allow‑list** where supported (Twilio).
* **2xx fast‑ack** (≤ 150ms) after enqueue; processing happens async.

**Idempotency & ordering**

* **EventStore** table with unique (provider, event\_id) and first\_seen\_at.
* Deduplicate regardless of retries; process **single‑thread per aggregate** (e.g., per donation\_id) to maintain order.
* **Replay** tool in Admin: pick event → reprocess.

**Processing**

* Normalize payload → domain command → write to **Outbox** (8.11) if further actions (notifications, indexing) are needed.
* On failure → exponential backoff (max 5 attempts) → **Dead‑Letter Queue** with reason.

**AC‑WH**

* AC‑WH‑1: All incoming events either **succeed**, get **retried**, or land in **DLQ** with a visible Admin alert.
* AC‑WH‑2: Stripe signature verification failures are dropped & logged (never processed).
* AC‑WH‑3: Operator can replay a single event or a range by time.

**7.17 Event catalog (selected mappings)**

**Stripe Payments**

* payment\_intent.succeeded → Create Donation; enqueue receipt (18); update Search index (16); update Leaderboard (12).
* payment\_intent.payment\_failed → Mark failed + notifier (email/SMS if action required).
* charge.refunded/refund.updated → Update donation/refund; send updated receipt; decrement progress.
* charge.dispute.created|closed → Create/update dispute record; reminders.

**Stripe Identity**

* identity.verification\_session.verified → KYC pass; publish gate may unlock (11).
* …requires\_input/…canceled → increment attempts; possible Compliance case.

**Stripe Connect**

* account.updated → requirements or capability changes → show banner; maybe selfie step‑up.
* payout.paid|failed|returned → Finance Ops queue update; notify organizer (18).

**SendGrid/Mailgun**

* delivered/open/click → DeliveryAttempt updates; bounce/complaint → SuppressionList add.

**Twilio SMS/Voice**

* DLRs → DeliveryAttempt updates; inbound STOP/HELP → preferences/suppressions update.

**Zendesk**

* ticket updates → Support view refresh; in‑app notification to user.

**IRS aggregator**

* (Poll) status → set org nonprofit badge.

**7.18 Monitoring, alerts & dashboards**

* **Providers health panel** (Admin 20.S): success %, latency, error codes, backlog sizes.
* Alerts:
  + Stripe webhook failure rate >2% (5‑min window)
  + SMS DLR <80% (hourly)
  + Email bounce spike >1% (daily)
  + AV scan failures >0.1% of uploads (daily)
  + DLQ non‑empty for >10 minutes

**On‑call runbooks** (tie to Section 21) for common incidents: Stripe outage, Twilio carrier issues, SendGrid blocklists, webhook backlog.

**7.19 Data model bindings (to Section 8)**

* donation.donation.processor\_id = payment\_intent or charge id.
* finance.refund.processor\_ref = Stripe Refund id.
* kyc.kyc\_profile status fields updated from Identity webhooks.
* kyc.kyb\_profile & payout\_eligibility from Connect.
* notif.delivery\_attempt from SendGrid/Twilio events.
* privacy.suppression\_list from SG/Twilio inbound.
* admin.audit\_log for replay actions / overrides.

**7.20 Acceptance Criteria (summary)**

* **Stripe**: Donations, refunds, disputes, Identity, Connect events are verified, idempotent, and produce correct domain changes & notifications.
* **Twilio**: OTP (Verify) works with voice fallback; STOP suppresses; DLRs reflected.
* **Email**: Template keys render; bounces/complaints → suppression; failover to Mailgun on outage.
* **Address**: Autocomplete & verification integrated; standardized data stored; non‑blocking warnings.
* **IRS**: Verified Nonprofit badge appears only on confirmed EIN + IRS match; monthly refresh.
* **Helpdesk**: Contact form creates tickets; status updates visible to users.
* **Media**: oEmbed enforced; safe fallbacks.
* **Storage/CDN**: Signed uploads, AV scan, only clean assets public.
* **CAPTCHA**: Applied at risk points; Admin‑tunable threshold.
* **Webhooks**: Signature verification, dedupe, DLQ, replay tools; processing within SLA.
* **Monitoring**: Provider dashboards live; alerts configured.

**7.21 Copy (out‑of‑box)**

* **Payout returned SMS:** “We couldn’t deliver your payout for **{campaign\_title}**. Update your bank details: {short\_link}”
* **Identity retry email:** “We couldn’t verify your ID. Try again in good lighting and include all four corners of your ID.”
* **Email bounce notice (user prefs):** “We couldn’t deliver messages to **{address}** due to a bounce. Update your email or re‑enable delivery.”

# 

# Section 8 — Database Schema

**Tech assumptions:** PostgreSQL 15+, UUID v7 IDs (or ULID), JSONB supported, timestamptz, amounts in **cents (int)** to avoid floating precision. Services emit domain events via an **Outbox** table.

## 8.0 Principles & Conventions

* **Namespaces:**  
  core (identity, orgs), campaign, donation, reward, team, wallet, kyc, mod, finance, notif, cms, search, analytics, admin, privacy, support, feature.
* **Column conventions:**  
  id UUID PRIMARY KEY, created\_at timestamptz NOT NULL DEFAULT now(), updated\_at timestamptz NOT NULL DEFAULT now(), status TEXT, ...\_id UUID FK.  
  Soft deletion via **status enums** (e.g., suspended, removed)—no hard deletes for money/PII.
* **Money:** amount\_cents INT NOT NULL, currency CHAR(3) NOT NULL DEFAULT 'USD'.
* **Slugs/usernames:** stored **lowercased**; citext for case‑insensitive match; unique constraints.
* **Privacy boundary:** **PII “Vault”** in schema privacy (email, phone, addresses). App tables store only **refs/tokens/statuses**. DSAR & suppression anchored here.
* **Audit:** All mutations of admin/staff actions, role/permission changes, payout overrides, template edits → admin.audit\_log.
* **RLS (Row Level Security):** Enabled for portal reads/writes on all user‑owned tables; staff bypass via role. Samples in §8.12.

## 8.1 High‑level domain map (ERD summary, textual)

* **core.user** 1—M **core.user\_email/phone**; 1—1 **privacy.user\_pii**; 1—M **campaign.campaign** (as organizer).
* **campaign.campaign** 1—M **team.member**, 1—M **reward.tier**, 1—M **donation.donation**, 1—M **finance.payout**, 1—M **mod.report**.
* **team.member** (lead/co‑lead/member) + **team.invite** + **team.referral\_link**; **donation** may attribute to team\_member\_id.
* **donation.donation** 1—0..1 **finance.refund**, 0..1 **donation.dispute**, 0..1 **reward.claim**; belongs to a **campaign** and **user (donor)**.
* **finance.wallet** per organizer; **payout** aggregates donations; **payout\_case** links approvals.
* **kyc.kyc\_profile/kyb\_profile** + **payout\_eligibility**.
* **notif.notification** + **notif.delivery\_attempt**; **message.thread** + **message.message**.
* **cms.page/section/asset**; **search.search\_index\_campaign** for discovery; **analytics.event** for telemetry.
* **admin.config/feature\_flag/experiment**; **admin.audit\_log**; **privacy.dsar**; **support.ticket** (pointer to helpdesk).

## 8.2 Tables by domain (fields & constraints)

### A) Identity & Accounts (core, privacy)

**core.user**

* id, username citext UNIQUE NOT NULL, display\_name text, joined\_at timestamptz, avatar\_ref text, role\_set jsonb (high‑level platform roles), gold\_badge bool.
* email\_primary\_id UUID FK -> core.user\_email(id); phone\_primary\_id UUID FK -> core.user\_phone(id).

**core.user\_email**

* id, user\_id, email citext UNIQUE, verified bool, verification\_sent\_at.
* **Constraint:** one verified = true must match email\_primary\_id.

**core.user\_phone**

* id, user\_id, e164 text UNIQUE, verified bool.
* **Constraint:** OTP flow audit in core.security\_log.

**privacy.user\_pii** (Vault)

* user\_id PK/FK, dob date, address\_book jsonb (USPS‑validated entries with labels), last4\_ssn text, stripe\_customer\_id text (token only).
* **RLS:** only owner & staff with PII role.

**core.security\_log**

* login, 2FA, device, IP, action, result.

**core.organization**

* id, org\_slug citext UNIQUE, name text, logo\_ref, website, verified\_org bool, verified\_nonprofit bool.
* **Memberships:** core.org\_member (user↔org).

**core.org\_member**

* id, org\_id, user\_id, role enum('admin','support'), scopes jsonb (campaign\_ids permitted), created\_by.

### B) Campaigns & Teams (campaign, team)

**campaign.campaign**

* id, organizer\_user\_id, org\_id NULL, title, short\_desc, story\_html, category, tags text[], city, state char(2),
* goal\_cents INT CHECK (goal\_cents >= 10000),
* funding\_model enum('KWR','AoN'),
* start\_date, end\_date,
* status enum('draft','live','ended','not\_funded','suspended','removed'),
* cover\_image\_ref, team\_enabled bool, leaderboard\_enabled bool.
* **Uniqs:** slug: slug citext UNIQUE.
* **Check:** end\_date ≥ start\_date; deadline windows per policy (4–12 weeks).

**team.member**

* id, campaign\_id, user\_id, role enum('lead','co\_lead','member'), joined\_at, removed\_at, referral\_code text UNIQUE, referral\_active bool.
* **Constraint:** **one** role='lead' per campaign; **≤1** co\_lead; **seat\_cap check** ≤5 via trigger.
* **Index:** (campaign\_id, role).

**team.invite**

* id, campaign\_id, email, role, token, expires\_at, accepted\_at, revoked\_at, status enum('pending','accepted','expired','revoked').

**team.support**

* Campaign Support seats (do not count toward 5).
* id, campaign\_id, user\_id, permissions jsonb, added\_by.

**team.referral\_link**

* id, campaign\_id, member\_user\_id, code text UNIQUE, url text, active bool.

### C) Media & Updates (campaign)

**campaign.media**

* id, campaign\_id, type enum('image','video','embed'), file\_ref or embed\_url, order\_index, alt\_text, size\_bytes.
* **Constraint:** limits (≤15 images, ≤5 videos) enforced by trigger.

**campaign.update**

* id, campaign\_id, author\_user\_id, body\_html, image\_ref, created\_at.
* **Constraint:** **1/day** per campaign (trigger).

### D) Rewards (reward)

**reward.tier**

* id, campaign\_id, tier\_number INT, amount\_min\_cents INT, name, desc\_html, delivery\_type enum('physical','digital'), est\_delivery\_month date,
* quantity\_limit INT NULL, options\_schema jsonb, shipping\_required bool, shipping\_region text.
* **Checks:** ascending amounts by (campaign\_id, tier\_number) via trigger; quantity\_remaining computed.

**reward.claim**

* donation\_id PK/FK, tier\_id, status enum('Unfulfilled','Pending','Processed'),
* contact jsonb, shipping\_address jsonb, options\_selected jsonb,
* tracking\_number text, donor\_visible\_note text, organizer\_private\_note text, updated\_by.
* **Index:** (tier\_id, status).

### E) Donations, Refunds, Disputes (donation, finance)

**donation.donation**

* id, campaign\_id, donor\_user\_id, amount\_cents, tip\_cents, fee\_cents, net\_to\_campaign\_cents,
* currency, is\_anonymous bool, hide\_name\_publicly bool,
* attribution\_member\_id NULL, funding\_model\_snapshot enum('KWR','AoN'),
* status enum('succeeded','refunded','aon\_auto\_refunded','failed'),
* processor\_id text (Stripe PaymentIntent/Charge id), created\_at.
* **Indexes:** (campaign\_id, created\_at DESC), (donor\_user\_id, created\_at DESC), partial WHERE status='succeeded'.

**finance.refund**

* id, donation\_id UNIQUE, amount\_cents, reason\_code enum('duplicate','donor\_request','reward\_issue','fraud','other'),
* approved\_by\_user\_id, approved\_by\_role, approved\_at, processor\_ref text, status enum('pending','sent','succeeded','failed').
* **Note:** Partial/Multiple refunds? If multi allowed, use separate **refund\_item** rows; we’ve aligned to **single aggregate** per donation with history in refund\_item.

**donation.dispute**

* id, donation\_id UNIQUE, opened\_at, deadline\_at, status enum('open','won','lost','closed'), evidence\_jsonb, processor\_ref.

**donation.attribution** (optional materialization)

* donation\_id, member\_user\_id, campaign\_id, utm jsonb, channel.

### F) Wallet & Payouts (finance)

**finance.wallet**

* id, organizer\_user\_id, org\_id NULL, balance\_available\_cents, balance\_on\_hold\_cents, balance\_reserved\_cents, updated\_at.

**finance.payout**

* id, campaign\_id, wallet\_id, amount\_cents, status enum('requested','in\_review','processing','paid','failed','returned','canceled'),
* requested\_at, processed\_at, paid\_at, returned\_reason text, statement\_memo text, destination\_token text (Stripe).

**finance.payout\_item**

* payout\_id, donation\_id, amount\_cents. (Snapshot for reconciliation.)

**finance.payout\_case**

* id, payout\_id, approvals jsonb (dual approvals), events jsonb, notes.

**finance.negative\_balance**

* id, wallet\_id, amount\_cents, age\_bucket enum('0\_7','8\_30','31\_60','60\_plus'), contact\_log jsonb.

### G) Identity & Verification (kyc)

**kyc.kyc\_profile**

* user\_id PK/FK, email\_verified bool, phone\_verified bool,
* id\_status enum('unstarted','verified','failed','manual\_review','selfie\_required'), id\_attempts\_24h,
* dob date, age\_verified bool, last\_selfie\_at.

**kyc.kyb\_profile**

* org\_id PK/FK, ein\_status enum('unstarted','verified','failed','manual\_review'), nonprofit\_status enum('unconfirmed','verified','failed'), irs\_last\_checked\_at.

**kyc.payout\_eligibility**

* user\_id or org\_id, bank\_status enum('unstarted','verified','mismatch'),
* compliance\_hold enum('none','publish','payout','reserve'), reserve\_pct INT, cooldown\_until timestamptz.

**kyc.compliance\_case**

* id, type enum('name\_mismatch','ein\_mismatch','sanctions\_hit'), entity (user|org), entity\_id, status, requested\_docs jsonb, notes, opened\_at,closed\_at.

**kyc.sanctions\_screening**

* entity\_type, entity\_id, screened\_at, result enum('clear','match','inconclusive'), provider\_ref.

### H) Messaging & Notifications (message, notif)

**message.thread**

* id, context enum('general','reward'), subject, created\_at, last\_msg\_at.

**message.participant**

* thread\_id, user\_id, role enum('sender','recipient'), muted bool, blocked bool, archived bool, PRIMARY KEY (thread\_id, user\_id).

**message.message**

* id, thread\_id, sender\_id, body\_html, attachment\_ref, created\_at, seen\_at.

**message.report**

* id, message\_id, reporter\_id, reason, created\_at, moderation\_case\_id.

**notif.notification\_event**

* id, type text, payload\_json jsonb, subject\_id, subject\_type, producer text, created\_at.

**notif.notification**

* id, user\_id, event\_id, topic, channels text[], status enum('queued','sent','suppressed','failed'),
* notification\_key text, quiet\_until timestamptz.

**notif.delivery\_attempt**

* id, notification\_id, channel, provider\_id, status, error\_code, sent\_at, delivered\_at, opened\_at, clicked\_at.

**notif.user\_preference**

* user\_id, topic, channel, enabled bool, quiet\_hours jsonb.

**notif.suppression**

* id, user\_id NULL, address text, channel, reason, added\_at.

### I) Moderation & Reports (mod)

**mod.report**

* id, campaign\_id, reporter\_user\_id, reasons text[], details text, attachments jsonb, created\_at.

**mod.case**

* id, campaign\_id, reason text, priority enum('P1','P2','P3'), status enum('open','needs\_changes','suspended','closed'),
* sla\_due, assignee\_user\_id, outcome\_code text, rationale text, history jsonb.

### J) Admin Config, Audit, Experiments (admin, feature)

**admin.audit\_log**

* id, actor\_user\_id, action\_type, target\_type, target\_id, before\_jsonb, after\_jsonb, ip, step\_up\_method, created\_at.

**admin.config**

* key text PRIMARY KEY, value\_jsonb, updated\_by.

**feature.feature\_flag**

* id, key text UNIQUE, on bool, rollout int, segments jsonb.

**feature.experiment**

* id, name, flags text[], variants jsonb, target jsonb, metrics text[], status enum('draft','running','stopped','rolled\_out').

### K) CMS & Discovery (cms, search)

**cms.page, cms.section, cms.asset, cms.publish\_log, cms.legal\_version**

* As defined in Section 9.17.

**search.search\_index\_campaign**

* campaign\_id, title, short\_desc, story\_excerpt, category, tags text[], city, state,
* status, funding\_model, verified\_user bool, verified\_org bool, nonprofit\_verified bool,
* goal\_cents, raised\_cents, pct\_funded, donors\_count,
* start\_date, end\_date, last\_update\_at,
* donation\_velocity\_24h, editors\_pick bool, team\_enabled bool, popularity\_score numeric,
* **Full‑text**: tsv tsvector (title + short\_desc + tags).
* **Indexes:** GIN on tsv, btree on (category,state,status).

**search.search\_index\_profile**

* Autocomplete store for user/org/team names.

**search.synonym\_set**, **search.ranking\_config** per Section 16.15.

### L) Analytics & Events (analytics)

**analytics.event**

* id, user\_id NULL, session\_id, name, campaign\_id NULL, metadata jsonb, created\_at.
* **Partitioned monthly**.
* **PII policy:** no raw email/phone; store only IDs/derived info.

**analytics.report**, **analytics.dashboard** (for builder definitions)—see Section 20.T.2.

### M) Support & KB (support)

**support.ticket\_stub** (reference to helpdesk)

* id, user\_id, external\_id, subject, status, created\_at, updated\_at.

**support.kb\_article\_stub**

* id, external\_id, path, title, updated\_at.

### N) Privacy & DSAR (privacy)

**privacy.dsar**

* id, user\_id, request\_type enum('export','delete','anonymize'), status, artifacts jsonb, completed\_at.

**privacy.suppression\_list**

* Mirror of notif suppression for cross‑channel privacy.

## 8.3 Sample DDL (PostgreSQL) — critical tables

(Representative snippets; apply to all tables with standard created\_at/updated\_at.)

-- core.user

CREATE TABLE core\_user (

id uuid PRIMARY KEY DEFAULT gen\_random\_uuid(),

username citext NOT NULL UNIQUE,

display\_name text,

joined\_at timestamptz NOT NULL DEFAULT now(),

avatar\_ref text,

role\_set jsonb NOT NULL DEFAULT '{}'::jsonb,

gold\_badge boolean NOT NULL DEFAULT false,

email\_primary\_id uuid,

phone\_primary\_id uuid,

created\_at timestamptz NOT NULL DEFAULT now(),

updated\_at timestamptz NOT NULL DEFAULT now()

);

-- campaign.campaign

CREATE TYPE funding\_model AS ENUM ('KWR','AoN');

CREATE TYPE campaign\_status AS ENUM ('draft','live','ended','not\_funded','suspended','removed');

CREATE TABLE campaign\_campaign (

id uuid PRIMARY KEY DEFAULT gen\_random\_uuid(),

organizer\_user\_id uuid NOT NULL REFERENCES core\_user(id),

org\_id uuid NULL REFERENCES core\_organization(id),

slug citext UNIQUE,

title text NOT NULL,

short\_desc text NOT NULL,

story\_html text NOT NULL,

category text NOT NULL,

tags text[] NOT NULL DEFAULT '{}',

city text NOT NULL,

state char(2) NOT NULL,

goal\_cents int NOT NULL CHECK (goal\_cents >= 10000),

funding\_model funding\_model NOT NULL,

start\_date date NOT NULL,

end\_date date NOT NULL,

status campaign\_status NOT NULL DEFAULT 'draft',

cover\_image\_ref text,

team\_enabled boolean NOT NULL DEFAULT true,

leaderboard\_enabled boolean NOT NULL DEFAULT false,

created\_at timestamptz NOT NULL DEFAULT now(),

updated\_at timestamptz NOT NULL DEFAULT now(),

CHECK (end\_date >= start\_date)

);

CREATE INDEX ON campaign\_campaign (status, end\_date);

CREATE INDEX ON campaign\_campaign (category, state);

-- team.member

CREATE TYPE team\_role AS ENUM ('lead','co\_lead','member');

CREATE TABLE team\_member (

id uuid PRIMARY KEY DEFAULT gen\_random\_uuid(),

campaign\_id uuid NOT NULL REFERENCES campaign\_campaign(id) ON DELETE CASCADE,

user\_id uuid NOT NULL REFERENCES core\_user(id),

role team\_role NOT NULL,

joined\_at timestamptz NOT NULL DEFAULT now(),

removed\_at timestamptz,

referral\_code text UNIQUE,

referral\_active boolean NOT NULL DEFAULT true,

created\_at timestamptz NOT NULL DEFAULT now(),

updated\_at timestamptz NOT NULL DEFAULT now()

);

CREATE INDEX ON team\_member (campaign\_id, role);

-- donation.donation

CREATE TYPE donation\_status AS ENUM ('succeeded','refunded','aon\_auto\_refunded','failed');

CREATE TABLE donation\_donation (

id uuid PRIMARY KEY DEFAULT gen\_random\_uuid(),

campaign\_id uuid NOT NULL REFERENCES campaign\_campaign(id),

donor\_user\_id uuid NOT NULL REFERENCES core\_user(id),

amount\_cents int NOT NULL CHECK (amount\_cents >= 500),

tip\_cents int NOT NULL DEFAULT 0,

fee\_cents int NOT NULL DEFAULT 0,

net\_to\_campaign\_cents int NOT NULL DEFAULT 0,

currency char(3) NOT NULL DEFAULT 'USD',

is\_anonymous boolean NOT NULL DEFAULT false,

hide\_name\_publicly boolean NOT NULL DEFAULT false,

attribution\_member\_id uuid NULL REFERENCES team\_member(id),

funding\_model\_snapshot funding\_model NOT NULL,

status donation\_status NOT NULL,

processor\_id text NOT NULL,

created\_at timestamptz NOT NULL DEFAULT now(),

updated\_at timestamptz NOT NULL DEFAULT now()

);

CREATE INDEX ON donation\_donation (campaign\_id, created\_at DESC);

CREATE INDEX ON donation\_donation (donor\_user\_id, created\_at DESC);

CREATE INDEX donation\_succeeded\_idx ON donation\_donation (campaign\_id) WHERE status='succeeded';

-- reward.tier & reward.claim

CREATE TYPE reward\_status AS ENUM ('Unfulfilled','Pending','Processed');

CREATE TABLE reward\_tier (

id uuid PRIMARY KEY DEFAULT gen\_random\_uuid(),

campaign\_id uuid NOT NULL REFERENCES campaign\_campaign(id) ON DELETE CASCADE,

tier\_number int NOT NULL,

amount\_min\_cents int NOT NULL CHECK (amount\_min\_cents >= 500),

name text NOT NULL,

desc\_html text,

delivery\_type text NOT NULL CHECK (delivery\_type IN ('physical','digital')),

est\_delivery\_month date,

quantity\_limit int,

options\_schema jsonb,

shipping\_required boolean NOT NULL DEFAULT false,

shipping\_region text,

created\_at timestamptz NOT NULL DEFAULT now(),

updated\_at timestamptz NOT NULL DEFAULT now(),

UNIQUE (campaign\_id, tier\_number)

);

CREATE TABLE reward\_claim (

donation\_id uuid PRIMARY KEY REFERENCES donation\_donation(id) ON DELETE CASCADE,

tier\_id uuid NOT NULL REFERENCES reward\_tier(id),

status reward\_status NOT NULL DEFAULT 'Unfulfilled',

contact jsonb,

shipping\_address jsonb,

options\_selected jsonb,

tracking\_number text,

donor\_visible\_note text,

organizer\_private\_note text,

updated\_by uuid REFERENCES core\_user(id),

created\_at timestamptz NOT NULL DEFAULT now(),

updated\_at timestamptz NOT NULL DEFAULT now()

);

-- finance.payout

CREATE TYPE payout\_status AS ENUM ('requested','in\_review','processing','paid','failed','returned','canceled');

CREATE TABLE finance\_payout (

id uuid PRIMARY KEY DEFAULT gen\_random\_uuid(),

campaign\_id uuid NOT NULL REFERENCES campaign\_campaign(id),

wallet\_id uuid NOT NULL REFERENCES finance\_wallet(id),

amount\_cents int NOT NULL CHECK (amount\_cents >= 0),

status payout\_status NOT NULL,

requested\_at timestamptz NOT NULL DEFAULT now(),

processed\_at timestamptz,

paid\_at timestamptz,

returned\_reason text,

statement\_memo text,

destination\_token text,

created\_at timestamptz NOT NULL DEFAULT now(),

updated\_at timestamptz NOT NULL DEFAULT now()

);

## 8.4 Referential integrity, constraints & policies

* **Team caps:** trigger team\_enforce\_seats() on team\_member insert/update to ensure ≤5 seats (lead+co\_lead+members) and ≤1 co\_lead.
* **Role conflicts (COI):** team\_member and team\_support enforce **mutual exclusivity** per campaign in trigger; accepting an invite to a conflicting role auto‑revokes the prior role (we write to admin.audit\_log).
* **Rewards ascending rule:** trigger on reward\_tier to enforce amount\_min\_cents(tier\_n) > tier\_{n-1}.
* **AoN not‑funded:** when campaign.status transitions to not\_funded, schedule refunds for all succeeded donations; mark donation.status='aon\_auto\_refunded'; freeze leaderboard & search index.
* **Payout eligibility:** check function gating finance\_payout insert/update based on kyc.payout\_eligibility (SSN/EIN + bank verified, no compliance hold, cooldown not active).
* **Invite single‑use & expiry:** team.invite token uniqueness; status auto‑sets to expired past expires\_at.

## 8.5 Indexing & performance plan

* **Hot paths:**  
  Donations by campaign/date; Rewards by campaign/status; Team leaderboard aggregates; Search index full‑text; Notifications by user; Messages by thread.
* **Recommended indexes:**
  + donation\_donation (campaign\_id, created\_at DESC) & partial on status.
  + reward\_claim (tier\_id, status); reward\_tier (campaign\_id, tier\_number).
  + team\_member (campaign\_id, role) & unique partial on (campaign\_id) WHERE role='lead'.
  + search\_index\_campaign tsv GIN + (category,state,status).
  + notif\_notification (user\_id, status); message\_message (thread\_id, created\_at DESC).
  + Time‑partition **analytics.event** monthly; BRIN on created\_at for large append‑only tables.
* **Materialized views (refresh every 5–15 min):**
  + mv\_team\_leaderboard (campaign\_id, member\_user\_id, amount\_cents, donations\_count, conv\_rate)
  + mv\_campaign\_progress (campaign\_id, raised\_cents, donors\_count, pct\_funded)
  + mv\_trending\_candidates (velocity with decay)

## 8.6 Search indexing pipeline

* **Triggers** on campaign, donation (status succeeded/refunded), reward\_tier, moderation state update → enqueue in admin.outbox.
* **Indexer service** consumes outbox → recompute tsv, popularity\_score, donation\_velocity\_24h → upsert search.search\_index\_campaign.
* SLA: trending reflects new donations within **≤15 minutes**.

## 8.7 Data privacy & retention

* **PII in privacy schema** only; access via whitelisted functions; never join raw emails in analytics.
* **Retention:**
  + admin.audit\_log 24 months;
  + notif.delivery\_attempt 12 months;
  + analytics.event 18 months (partition drop policy);
  + **DSAR**: privacy.dsar orchestrates exports/anonymization; donations remain but donor display may be anonymized per policy.
* **Anonymization:** swap display\_name on donation receipts view; keep donor\_user\_id for accounting but hide publicly if is\_anonymous or DSAR anonymize executed.

## 8.8 Security & RLS examples

* **Portal RLS** (example for donations): user can SELECT their own donations or donations in campaigns they **own** (organizer) in **Organizer Analytics** views.

ALTER TABLE donation\_donation ENABLE ROW LEVEL SECURITY;

CREATE POLICY donor\_reads ON donation\_donation

FOR SELECT TO portal\_user

USING (donor\_user\_id = current\_setting('app.user\_id')::uuid);

CREATE POLICY organizer\_reads ON donation\_donation

FOR SELECT TO portal\_user

USING (campaign\_id IN (

SELECT id FROM campaign\_campaign WHERE organizer\_user\_id = current\_setting('app.user\_id')::uuid

));

* **Staff bypass** via role staff\_user on a separate connection role; all staff actions mirrored in admin.audit\_log.

## 8.9 Invariants & integrity checks (AC)

* **Unique lead per campaign** (team\_member partial unique).
* **Max one co‑lead** per campaign (trigger).
* **≤5 seats** per campaign team (trigger across roles).
* **Reward tier ascending** enforced.
* **Donation amount ≥ $5**; whole dollars validated at app layer; DB check uses amount\_cents % 100 = 0.
* **AoN refunds** executed for not‑funded; donation statuses consistent.
* **Refund ≤ donation amount** minus previous refunds; check constraint or trigger.
* **Payouts** include only donations not already paid out; enforce via finance.payout\_item uniqueness on donation\_id.

## 8.10 Views for product & admin

* view\_public\_campaign (joins campaign + organizer badges + mv\_progress).
* view\_public\_profile\_stats (from profile\_stats\_cache, §10.W).
* view\_organizer\_wallet\_summary (eligible/on\_hold/reserved/net\_available).
* view\_team\_attribution (donations with member link, anonymized PII).
* view\_moderation\_overview (reports + cases + SLA).

## 8.11 Outbox & notifications

**admin.outbox**

* id, topic, payload\_jsonb, created\_at, processed\_at NULL.
* Producers write once; consumers mark processed\_at.
* Topics: search.campaign\_upsert, notif.event, analytics.event, finance.payout\_status\_changed.

## 8.12 Partitioning & storage notes

* **High‑volume tables**: analytics.event, notif.delivery\_attempt, message.message → monthly partitions.
* **Archive tables** for ended campaigns older than N months (optional), with **read‑only** flags.

## 8.13 Example queries (operational)

* **Leaderboard (materialized or on demand):**

SELECT tm.user\_id, SUM(d.amount\_cents) AS raised\_cents, COUNT(\*) AS donations

FROM donation\_donation d

JOIN team\_member tm ON d.attribution\_member\_id = tm.id

WHERE tm.campaign\_id = $1 AND d.status='succeeded'

GROUP BY tm.user\_id

ORDER BY raised\_cents DESC;

* **Eligible for payout:**

SELECT campaign\_id, SUM(net\_to\_campaign\_cents) - COALESCE(SUM(paid.amount\_cents),0) AS eligible\_cents

FROM donation\_donation d

LEFT JOIN finance\_payout\_item paid ON paid.donation\_id = d.id

WHERE d.campaign\_id=$1 AND d.status='succeeded'

GROUP BY campaign\_id;

## 8.14 Migration & seeding plan

* **Phase‑0:** core user, email/phone, security\_log, orgs.
* **Phase‑1:** campaigns, team, media, rewards, donations.
* **Phase‑2:** wallet/payout, refunds/disputes, kyc profiles.
* **Phase‑3:** messaging, notifications, moderation.
* **Phase‑4:** cms, search index, analytics, admin config, feature flags.

Seed: categories (12), report reasons, default tip/fee configs, message abuse reasons.

## 8.15 Monitoring & health

* **PG bloat & vacuum** dashboards;
* Replication lag alarms;
* Slow query log;
* Background job failures (outbox consumer);
* Storage thresholds for partitions.

## 8.16 Summary Acceptance Criteria (DB level)

* All FK relationships present with sensible ON DELETE behavior (mostly RESTRICT for money; CASCADE for team/media).
* Constraints enforce business rules (seats, ascending tiers, donation min, payout uniqueness).
* Privacy partition implemented (privacy schema) and RLS policies on user‑owned tables.
* Indexes in place for hot paths; partitions for heavy write paths.
* Outbox present; search index upserts within SLA.
* Audit coverage on staff/admin mutations.
* DSAR path supported (export/anonymize without data loss in financial history).

**Section 9 — Marketing CMS & Public Pages**

**9.0 Scope & dependencies**

**Scope:** Public pages & components (Home, About, Contact, Knowledge Base, Legal/Policy, Press, System pages), CMS authoring workflow, preview/scheduling/versioning, asset library, accessibility/performance budgets, SEO/OG/JSON‑LD, experiments, analytics, and admin governance.  
**Depends on:** Section 16 (Discovery/search), 20.O (Theme/Copy library/OG editor), 20.P (SEO/Ranking/Redirects), 18 (Notifications), 10 (Public profiles & DM), 20.G (Helpdesk/KB integration).

**9.1 Page inventory & routing**

* **Home:** /
* **About:** /about
* **Contact:** /contact
* **Knowledge Base:** /help (index) and /help/{category}/{article-slug}
* **Legal/Policy:** /terms, /privacy, /community-guidelines, /refunds, /security, /accessibility
* **Press/Media:** /press
* **Careers** *(optional Phase‑2)*: /careers
* **System pages:** /404, /410, /500, /maintenance
* **Status (optional link to external statuspage):** /status (redirect)

**AC‑ROUTING‑1:** All pages SSG/SSR with canonical tags; 301 legacy paths configurable in Admin Redirects (20.P).

**9.2 Roles, permissions & workflow (CMS governance)**

**Roles:**

* **Author:** create/edit drafts; cannot publish.
* **Editor:** edit/review; request changes; schedule.
* **Publisher:** publish/schedule/rollback (non‑legal).
* **Legal Publisher:** publish/schedule/rollback **legal/policy** pages.
* **Designer:** theme assets (20.O), image crops, OG templates.
* **Super Admin:** all actions + feature flags.

**Workflow:**

1. **Draft → Review → Approved → Publish (now/scheduled)**.
2. **Legal pages** require **two‑person approval** (Editor + Legal Publisher).
3. **Preview**: tokenized URL (?preview=1&v={draftId}) sharable internally; expires in 7 days.

**AC‑WF‑1:** Cannot publish if **accessibility checks fail** (missing alt text, low contrast hero overlays).  
**AC‑WF‑2:** All publishes/rollbacks are **audited** (20.K).

**9.3 Asset & media library**

* Upload: jpg/png/webp/svg (logos/icons) with **auto‑WebP** renditions and responsive sizes.
* Required metadata: **alt text**, copyright/credit, license.
* Tools: cropper; focal point; background overlay (for hero); file size hard caps (images ≤ 5 MB; logos ≤ 512 KB).
* Storage: CDN with versioned URLs and immutable cache headers.

**AC‑ASSET‑1:** Block publish if an image lacks alt text (except purely decorative with role="presentation").  
**AC‑ASSET‑2:** OG images generated via 20.O template respect safe text margins.

**9.4 Component library (page builder blocks)**

All components are **content‑safe** (no arbitrary HTML/JS). Copy strings should preferentially use the **Copy Library** (20.O.F) keys where appropriate.

1. **Hero** (variants: Image, Video, Gradient, Minimal)
   * Fields: Headline, Subhead, Primary CTA (label/link), Secondary CTA (optional), Background (image/video), Dark overlay toggle.
   * AC: Enforce 1–2 line clamp on H1; mobile crop preview; buttons keyboard‑focusable.
2. **Feature Grid / Curated Row**
   * 3–4 cards per row; manual selection of campaigns or static links.
   * AC: Card titles 2‑line clamp; grid responsive (3/2/1).
3. **Dynamic Campaign Shelf**
   * Data‑driven (Trending, Ending soon, Recently launched) mirroring Section 16; optional “Show more” link.
   * AC: Respects Admin ranking knobs and cache windows.
4. **Categories Carousel**
   * 12 primary categories with icons; link to /category/{slug}.
   * AC: Keyboard scroll controls & ARIA labels.
5. **How It Works (Steps 1‑3/1‑4)**
   * Icon, Title, Body; optional CTAs per step.
   * AC: Steps are ordered list (<ol>) for screen readers.
6. **Testimonials Carousel**
   * Quote, Name, Role (e.g., “Organizer”), optional avatar.
   * AC: Do not autoplay; manual controls visible to SR.
7. **Stats Band**
   * KPIs: total raised, campaigns launched, donors; animated count‑up (reduced‑motion respects user setting).
   * AC: Numbers read as text for SR.
8. **Press Logo Strip**
   * Logos with links to articles.
   * AC: Provide aria-label describing outlet.
9. **Call‑to‑Action Band**
   * Big CTA (e.g., “Start a campaign”), small supporting text.
   * AC: Contrast ≥ 4.5:1.
10. **Text + Media**
    * Rich text block with left/right image/video.
    * AC: Media has captions/alt; non‑autoplay video.
11. **FAQ Embed**
    * Select KB category or custom Q/A list.
    * AC: Uses <details>/<summary> or ARIA‑compliant accordion.
12. **Newsletter Signup** *(Phase‑2)*
    * Email field + consent checkbox; integrates with ESP.
13. **Contact Card Grid**
    * Cards: Donations support, Organizer support, Press, Legal. Each links to /contact with prefilled category.
14. **Social Proof Mosaic**
    * Organizer avatars/donor first‑names list; anonymized.
15. **Announcement Banner** (site‑wide; 20.O)
    * Dismissible; scheduling; audience targeting.

**9.5 Home page blueprint (default composition)**

Order (editable in CMS):

1. **Hero** (Start a campaign / Browse campaigns)
2. **Trending now** (Dynamic shelf)
3. **How it works** (3 steps)
4. **Editor’s Picks** (Curated row)
5. **In your state** (if user consents; else Recently launched)
6. **Categories carousel**
7. **Verified nonprofits** (dynamic shelf filtered by badge)
8. **Stats band**
9. **Testimonials**
10. **CTA band**

**AC‑HOME‑1:** LCP element (Hero image or first card) ≤ 2.5s on mid‑range mobile, CLS ≤ 0.1.  
**AC‑HOME‑2:** If no curated picks exist, component auto‑hides and compacts spacing.

**9.6 About page blueprint**

Sections:

* **Mission & values** (Text + Media)
* **Our impact** (Stats band + case studies)
* **Trust & Safety** (link to Community Guidelines and Security pages)
* **Team & leadership** *(optional Phase‑2; portraits with bios)*
* **Press highlights** (Press logo strip)
* **CTA band** (“Join as an organizer”)

**AC‑ABOUT‑1:** Headings follow a single H1 then H2/H3 structure; images have alt; portraits marked decorative if no essential info.

**9.7 Contact page blueprint**

**Purpose:** Route users to the right support channel, reduce load via KB suggestions.

Sections:

* **Smart contact form** (integrates with helpdesk; Section 20.G)
  + Fields: Name, Email, Phone (optional), Category (Donation / Organizer / Account / Verification / Trust & Safety / Press / Legal), Subject, Message, Attachments (pdf/jpg/png ≤ 5 MB).
  + Logic: Suggest relevant KB articles inline as user types; if user selects an article, show **“Still need help?”** → continue to form.
  + Submission: creates ticket with metadata (URL referrer, user\_id if logged in).
* **Phone support** (hours & timezone)
* **AI Chatbot** launcher (embedded widget)
* **For press**: link to /press
* **For security reports**: link to /security disclosure policy

**AC‑CONTACT‑1:** Form uses honeypot + time‑to‑complete spam checks; rate‑limited (Section 18 & 20.M).  
**AC‑CONTACT‑2:** On success, show case ID + expected SLA.

**9.8 Knowledge Base (front‑end)**

**Index /help:**

* Search bar (typeahead), categories grid, “Popular this week,” “Getting started,” “Trust & Safety.”
* Content source: helpdesk/KB integration from 20.G (versioned, scheduled).

**Article page /help/{category}/{slug}:**

* Title, updated date, read time, breadcrumbs, article body, “Was this helpful?” (Yes/No) with optional comment.
* Side rail: related articles; “Still need help?” CTA to contact form.
* Structured data: FAQPage if article contains Q/A blocks.

**AC‑KB‑1:** Article feedback writes to KB analytics; excessive “Not helpful” triggers review task in Admin.  
**AC‑KB‑2:** Code blocks (if any) are copyable and accessible.

**9.9 Legal & policy pages**

Pages: **Terms**, **Privacy**, **Community Guidelines**, **Refunds**, **Security**, **Accessibility**.

* **Two‑person publish** (Editor + Legal Publisher).
* **Versioning:** show **Effective date**, link **View previous versions** (modal with changelog).
* **Anchored sections** with ToC sidebar; deep‑links preserved.

**AC‑LEGAL‑1:** Every legal page footer has “Last updated {date}”.  
**AC‑LEGAL‑2:** Publishing notifies subscribers of policy updates (optional; Section 18).

**9.10 Press page**

* Media kit: logos (PNG/SVG), brand guide PDF.
* Press contacts (email/phone), latest coverage (links).
* Featured stats (pull from Stats band).

**AC‑PRESS‑1:** Assets downloadable; license terms shown.

**9.11 System pages**

* **404 Not Found:** Search box, popular categories, link Home.
* **410 Gone:** “This page is no longer available” + browse links.
* **500 Error:** Apology, retry CTA, Support link.
* **Maintenance:** Reason + ETA; donations disabled (ties to 20.O Maintenance Mode).

**AC‑SYS‑1:** All system pages render with main header & footer disabled to reduce confusion; include logo & essential links.

**9.12 Accessibility & performance (public pages)**

* **WCAG 2.2 AA** across all components.
* Respect **prefers‑reduced‑motion**.
* Keyboard focus outlines; ARIA roles for carousels/accordions.
* Performance budgets (4G mid‑range mobile): LCP ≤ 2.5s, CLS ≤ 0.1, TBT ≤ 200ms.
* Images: responsive srcset, lazy‑load below the fold, preconnect to CDN.

**AC‑A11Y‑1:** Accessibility linter must pass before publish.  
**AC‑PERF‑1:** CMS warns if a hero image exceeds 500 KB on mobile rendition.

**9.13 SEO & structured data**

* Unique **title/meta** per page; OG tags via 20.O OG editor.
* **JSON‑LD**: WebSite + SearchAction on Home; BreadcrumbList on KB/Legal; Organization on About/Press.
* **Sitemaps** include /help/\*, /legal/\* (Terms, Privacy, …).
* Robots: allow public; disallow /admin/\*, /portal/\*, /api/\*.

**AC‑SEO‑1:** CMS enforces meta description length (≤ 160 chars) and title length (≤ 60 chars).  
**AC‑SEO‑2:** 301 redirects configurable per page; canonical field available.

**9.14 Experiments & personalization (hooks)**

* Any component can be put behind a **feature flag** or **A/B test** (20.Q): Hero variant, CTA copy, carousel order, stats band presence.
* “In your state” personalization respects geolocation consent.

**AC‑EXP‑1:** Experiment requires primary metric (e.g., “Start campaign clicks”), stop criteria, and ramp plan.

**9.15 Analytics & events**

* Track per‑component impressions & clicks: hero\_cta\_click, feature\_card\_click, category\_click, contact\_form\_submit, kb\_article\_view, kb\_feedback\_submit.
* Funnel: home\_view → browse\_category/search → campaign\_view → donate\_start.
* KB search analytics: queries, zero‑result rate.

**AC‑ANL‑1:** All events carry page\_type, component\_key, and UTM passthrough when relevant.

**9.16 Copy kit (public pages)**

**Hero defaults**

* Headline: “Fund hope. Fund change.”
* Subhead: “Start a campaign or support one today.”

**How it works (3‑step)**

* Step 1: “Create your campaign” — “Share your story, goal, and photos.”
* Step 2: “Share with your community” — “Invite friends, family, and teammates.”
* Step 3: “Receive donations securely” — “Stripe‑powered payments. Payouts when your campaign ends.”

**Contact confirmation**

* “Thanks—your message was sent. We’ll reply within **1 business day**. Case ID: **{id}**.”

**404**

* “We couldn’t find that page.” — “Try searching or explore campaigns.”

**9.17 Data model (conceptual CMS objects)**

* **Page**: id, path, title, meta\_title, meta\_desc, canonical\_url, status {draft|scheduled|published}, scheduled\_at, published\_at, version\_id, preview\_token, legal\_flag (bool), requires\_two\_person (bool)
* **Section**: id, page\_id, position, type (hero|feature\_grid|dynamic\_shelf|... ), config\_json, enabled
* **Asset**: id, url, kind (image|video|svg|pdf), alt, credit, license, width, height, size\_bytes, focal\_point
* **PublishLog**: id, page\_id, action (publish|rollback|schedule), actor\_id, diff\_json, created\_at
* **LegalVersion**: id, page\_id, effective\_date, diff\_summary, body\_html
* **KbArticle** (pointer to helpdesk id for rendering)
* **ExperimentBinding**: id, page\_id or section\_id, flag\_key, variant, start\_at, end\_at, metric\_key
* **Redirect** (from 20.P): from\_path, to\_path, code (301|302)

**9.18 Acceptance Criteria (summary)**

* **Authoring:** Draft/review/publish with preview and schedule; two‑person approval for legal pages; audit trail.
* **Assets:** Alt text required; focal point & renditions; OG images via template.
* **Components:** All blocks responsive, accessible, and performance‑friendly; default Home composition provided; dynamic shelves powered by Section 16 ranking.
* **Contact:** Helpdesk integration with smart suggestions; spam/rate‑limit; SLA displayed.
* **KB:** Searchable, browsable, “helpful” rating stored; related articles; structured data added when appropriate.
* **Legal:** Version history with effective dates; deep‑link anchors; user notification optional.
* **System pages:** Helpful, branded, and accessible; maintenance ties to Admin Maintenance Mode.
* **SEO:** Titles/meta/JSON‑LD/canonicals validated; sitemaps include KB/Legal; redirects manageable.
* **Analytics:** Per‑component events; KB analytics; funnel instrumentation.
* **Experiments:** Hooked up to 20.Q; guardrails enforced.
* **Accessibility & Performance:** WCAG 2.2 AA; LCP/CLS/TBT budgets met; pre‑publish checks block regressions.

**9.19 Roadmap (Phase‑2)**

* **Blog** (stories from organizers), with author profiles and tags.
* **Localization** (ES first) with language switcher; hreflang tags.
* **Server‑side personalization** for logged‑in users on Home (“For you” shelf).
* **Dynamic press quotes** pulled from a CMS collection.
* **KB sandbox** for AI summaries (with human review before publish).

# Section 9B — CMS & Marketing Site

**Scope:** Everything that renders outside the logged‑in portal/admin experience: the **marketing site** (Home, About, Contact, Knowledge Base landing & articles), **public legal documents**, and editorial control for **discovery rails** callouts. Includes a **headless CMS** spec (content types, roles, states), **preview & publish** flow, **redirects**, **OG image automation**, and **site‑wide navigation**.

**Assumptions:**  
US‑only service, English‑only MVP (strings externalized per §4.10). No third‑party trackers beyond first‑party analytics; marketing pixels off by default (§6.4).

## 9.0 Site architecture & routing

* **Base domain:** www.{brand}.com (marketing + public pages).
* **App/portal:** app.{brand}.com (or /app route) for logged‑in experience.
* **Routes (marketing):**
  + / (Home)
  + /about
  + /contact
  + /help (KB hub)
  + /help/{category}/{article-slug} (KB article)
  + /legal/{doc-slug} (Terms, Privacy, Refunds, Community, Security, Accessibility, Sub‑processors)
  + /discover/\* and /search (spec §16; visible from marketing nav)
  + Catch‑alls: /404, /410, /500
* **Rendering strategy:**
  + **Hybrid SSR/SSG**: Above‑the‑fold modules **SSR**; content fetched from **headless CMS**.
  + **Cache:** CDN with **stale‑while‑revalidate (60s)** for pages; instant purge on publish.
  + **Safety:** Sanitizer strips inline scripts; embeds limited to approved providers (YouTube/Vimeo).

## 9.1 CMS roles & permissions (ties to §20 Admin)

| **Role** | **Create/Edit** | **Submit for Review** | **Approve/Publish** | **Legal Docs Publish** | **Redirects** | **Menus/Nav** | **Templates** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Author** | Pages, KB, Posts | ✅ | ❌ | ❌ | ❌ | ❌ | ❌ |
| **Editor** | All content types | ✅ | ✅ (non‑Legal) | ❌ | ✅ | ✅ | ✅ |
| **Legal Reviewer** | Legal docs only | ✅ | ✅ (co‑approve) | ✅ (requires 2‑person) | ❌ | ❌ | ❌ |
| **Publisher** | All | ✅ | ✅ | ❌ (needs Legal) | ✅ | ✅ | ✅ |
| **Admin** | All + system | — | — | ✅ | ✅ | ✅ | ✅ |

**Two‑person rule (Legal):** Legal docs require **Editor/Publisher + Legal Reviewer** to publish (§6.10). All content edits audited in admin.audit\_log.

## 9.2 Content types (schemas)

### 9.2.1 ****Page****

* title, slug, status (draft|in\_review|scheduled|published|archived), scheduled\_at, seo\_title, seo\_description (≤160), hero (image\_ref, alt), modules[], og\_image\_mode ('auto'|'custom'), og\_image\_ref?, noindex bool, last\_reviewed\_at, changelog[] (who, what)

### 9.2.2 ****Module**** (block library)

* **Hero** (headline, subhead, CTA link)
* **TextMedia** (rich text + left/right image/video)
* **Stats** (icon/number/label triplets)
* **Testimonials** (quote, name, role)
* **FAQList** (Q/A pairs; converts to FAQPage schema if used alone)
* **FeatureGrid** (cards with icon/title/body/CTA)
* **DiscoveryRail** (injects one of §16 rails or a curated list)
* **CTA\_Banner** (single CTA)
* **KB\_Promo** (links into KB categories)
* **LegalTOC** (auto‑generates ToC from headings on legal pages)

All modules consume **design tokens** (§4.1) and pass **a11y** checks (focus, headings, alt text).

### 9.2.3 ****KB Article****

* title, slug, category, subcategories[] (≤2 deep), status, seo\_title, seo\_description, body\_rte, author, last\_updated\_at, related\_articles[], faq\_items[] (optional), search\_synonyms[], estimated\_read\_min, helpfulness: {yes, no, feedback\_text?, email\_optional?}

### 9.2.4 ****Legal Document****

* title, slug, status, effective\_date, version, body\_rte (legal-safe subset), prior\_versions[] (version, effective\_date, link)

### 9.2.5 ****Redirect****

* from\_path, to\_url, type (301|302), start\_at?, end\_at?, notes, created\_by

### 9.2.6 ****Menu / Navigation****

* header\_links[] (label, url, order, rel? target?)
* footer\_links[] (label, url, section group: Company, Legal, Help, Social)

### 9.2.7 ****Media Asset****

* file\_ref, alt\_text, caption?, copyright?, width, height, size, srcset[], focal\_point

### 9.2.8 ****Copy Library Key**** (optional, non‑dev copy)

* key, scope (marketing|legal), text, notes, owner, last\_updated\_at

## 9.3 Editorial workflow & states

**States:** draft → in\_review → scheduled|published → archived.

* **Draft:** editable by Author/Editor.
* **In\_review:** locked; Editor/Publisher reviews; **Legal** participates for legal docs.
* **Scheduled:** go live at scheduled\_at (timezone aware).
* **Published:** visible; new versions create a **diff** and version bump.
* **Archived:** 410 or kept behind noindex (configurable); Legal pages keep prior versions accessible.

**Notifications (§18):**

* Submit for review → notify Editors;
* Approved → notify Authors;
* Scheduled → notify Publisher 1h before publish;
* Publish → purge cache; notify Slack/email (internal).

**Preview:**

* Unique **preview token** appended to URL; expires in 24h; shares exact rendering.
* Editor can generate a **public preview link** (noindex) for stakeholders.

## 9.4 Landing pages (content & modules)

### 9.4.1 ****Home (/)****

**Goal:** conversion into discovery and create‑a‑campaign.

**Recommended module order (editable):**

1. **Hero**: H1 (“Raise funds, safely and simply”); subhead; CTA “Start a campaign” (to app) and secondary “Find fundraisers” (→ /discover).
2. **DiscoveryRail**: “Trending near you” (auto) with 8 cards (from §16).
3. **TextMedia**: “How it works” (3 steps: Create → Share → Get paid).
4. **Stats**: “$X raised”, “Y donors”, “Z verified organizers” (dynamic, cached).
5. **FeatureGrid**: “Why choose us” (KYC & safety, simple rewards, team fundraising).
6. **Testimonials** (optional; curated quotes).
7. **KB\_Promo**: “Learn more: FAQs, fees, safety” links to KB categories.
8. **CTA\_Banner**: secondary conversion.

**SEO:** H1 unique, meta description; structured WebSite schema with SearchAction.

**A11y:** Hero buttons in natural tab order; contrasts per §4.

### 9.4.2 ****About (/about)****

* Modules: Mission (TextMedia), Team (grid), Trust & Safety (TextMedia), Press mentions (logos), Contact CTA.
* Optional: Timeline module (Phase‑2).

### 9.4.3 ****Contact (/contact)****

* **Form fields:** name, email, phone (optional), topic (Support/Billing/Trust & Safety/Partnerships), message (max 2,000).
* **Guards:** hCaptcha, rate limit 3 submissions/day/IP; profanity filter.
* **Routing:** Creates **Support ticket** (Section 20.G) with topic routing; autoresponder (18.J).
* **Success state:** friendly confirmation; SLA copy.
* **A11y:** Labels & aria-describedby; error summary on submit.

### 9.4.4 ****Knowledge Base (/help)****

* **Hub:** categories (cards) with article counts; search bar with typeahead; “Popular” and “New” rails.
* **Article page:**
  + H1 title; “Last updated” date; reading time; author.
  + Body RTE (safe subset); **on‑page ToC** if > 3 headings.
  + **FAQ items** render as accordions; apply FAQPage schema if present.
  + **Helpful?** Yes/No with **feedback** (free text, optional email).
  + **Related articles** list; breadcrumb nav to category.
  + **Report issue** link → Support ticket with article context.
* **Search:** highlights matches; synonyms from KB schema; result cards show snippet; keyboardable.
* **A11y:** Headings hierarchical; code snippets (if any) wrapped accessibly; images with alt.

### 9.4.5 ****Legal (/legal/{doc})****

* Documents: **Terms**, **Privacy**, **Community Guidelines**, **Refunds**, **Security**, **Accessibility**, **Sub‑processors**.
* **Two‑person approval** required (§6.10).
* **Effective date** banner; **version selector** dropdown; clear change log.
* **Anchored ToC**; “Last updated” inside page; **print styles** (§4.12).
* **DPA/Sub‑processor** page pulls from Admin registry (§6.1).
* **Re‑consent:** when flagged, triggers notification (§18) and portal re‑consent prompt (Phase‑2).

## 9.5 Navigation, header/footer

* **Header:** Logo → Home; Nav links: Discover, How it works, Pricing (if you expose), About, Help; “Start a campaign” CTA (to app).
* **Footer:** Company (About, Careers [placeholder], Press [optional]), Help (KB, Contact), Legal (Terms, Privacy, Refunds, Community, Security, Accessibility, Sub‑processors), Social links.
* **Behavior:** Sticky header, reduces height on scroll; focus ring visible; skip link “Skip to content”.

## 9.6 SEO & structured data (marketing)

* Titles & meta descriptions per page; enforce ≤ 60 chars title, ≤ 160 desc.
* **Canonical** on each page; **OpenGraph/Twitter** tags.
* **OG images:**
  + **Auto generator**: dynamic image with title, brand, cover (for Pages with hero).
  + **Custom upload** optional; validate 1200×630.
* **Schema.org:**
  + WebSite (+ SearchAction on Home), Organization (Contact page), FAQPage (FAQ modules), Article for KB articles.
* **Sitemaps:** sitemap.xml with pages, categories, KB articles, legal; lastmod on updates; split by type if >5k URLs.
* **Robots:** allow crawl except: preview URLs, archived pages (410), any noindex flagged.

## 9.7 Performance & accessibility (budgets per §4)

* **Budgets (marketing pages):** LCP ≤ **2.5s**, CLS ≤ **0.10**, TBT ≤ **200ms**, JS ≤ **170KB** gz, CSS ≤ **50KB** gz.
* **Images:** AVIF/WebP + srcset; hero ≤ 500KB mobile rendition; lazy load below fold.
* **Fonts:** system stack preferred; if custom, **single WOFF2**, font-display: swap.
* **A11y:** color contrast AA; keyboard focus; headings present and ordered; media alt text required; FAQ accordions keyboardable.
* **Reduced motion:** disable parallax/scroll effects when requested.

## 9.8 Security & content safety

* **Sanitizer:** strips scripts/iframes; allowlist embeds (YouTube/Vimeo) only.
* **Links:** force https, add rel="nofollow noopener"; strip UTM/tracking on inbound save to copy fields.
* **Uploads:** AV scan; EXIF strip; size caps with informative errors.
* **Forms:** CSRF tokens; hCaptcha; server rate limits and IP throttles; store logs (minimal PII).
* **No P0 data** allowed in CMS fields (no SSNs, tokens).

## 9.9 Admin CMS console (ties to §20.H)

* **Content index** with filters (type, author, status, scheduled, changed since).
* **Editor** with side‑by‑side preview; mobile preview toggle; accessibility hints (heading levels, alt check).
* **Workflow pane**: assign reviewer, add notes, request changes, approve, schedule.
* **Legal workspace**: diff viewer; two‑person publish gate; version/effective date controls; prior versions list.
* **Redirect Manager**: add/edit/bulk import CSV; conflict detection; test tool; 301/302; date‑bounded.
* **Menus**: drag‑drop; link validator.
* **OG image generator**: choose auto/custom; preview.
* **KB manager**: category tree editor; related article picker; helpfulness dashboard; broken link checker.
* **Discovery rails controls**: insert curated card lists (IDs) or pick a rail from §16; schedule; per‑rail A/B variant tag.
* **Audit log**: who/what/when diff for each publish.

## 9.10 Data model (additions to §8)

cms.page

- id, title, slug, status, scheduled\_at, seo\_title, seo\_description, hero\_ref, modules\_jsonb,

og\_image\_mode, og\_image\_ref, noindex bool, last\_reviewed\_at, created\_by\_id, updated\_by\_id, created\_at, updated\_at

cms.kb\_article

- id, title, slug, category, subcategories jsonb, status, seo\_title, seo\_description, body\_html, author\_id,

last\_updated\_at, related\_article\_ids jsonb, search\_synonyms jsonb, estimated\_read\_min int

cms.legal\_doc

- id, title, slug, status, version, effective\_date, body\_html, prior\_versions jsonb

cms.redirect

- id, from\_path, to\_url, type, start\_at, end\_at, notes, created\_by\_id, created\_at

cms.menu

- id, location ('header'|'footer'), items jsonb [{label,url,order,external,rel,target}]

cms.media\_asset

- id, file\_ref, alt\_text, caption, copyright, width, height, size\_bytes, srcset jsonb, focal\_point jsonb, uploaded\_by\_id

cms.copy\_key

- id, key, scope, text, notes, owner\_id, updated\_at

cms.review

- id, content\_type, content\_id, from\_status, to\_status, requested\_by\_id, assignee\_id, note, created\_at, resolved\_at

## 9.11 Acceptance Criteria (summary)

1. **Roles & workflow:** Authors create; Editors review/publish; Legal docs require two‑person approval with effective dates and version history.
2. **Pages & modules:** Home/About/Contact/KB/Legal can be built from module library; modules use design tokens; pass a11y checks.
3. **KB:** Categories & articles searchable; article template supports ToC, FAQ, helpfulness voting, related articles, and support escalation.
4. **Contact form:** routes to Support with topic mapping; CAPTCHA & rate limits; autoresponder sent.
5. **SEO/OG:** Titles/meta/canonicals generated; OG image auto/custom; sitemaps produced; robots respected; structured data valid.
6. **Performance:** Budgets met on Home, About, KB article; images optimized; fonts swapped.
7. **Security:** Content sanitized; allowed embeds only; AV scan on uploads; links hardened.
8. **Redirects & menus:** Configurable in Admin; conflicts prevented; 301/302 supported.
9. **Publishing:** Preview links work; scheduled publish honors timezone; CDN purged on publish; audit logs capture all changes.
10. **Discovery rails:** CMS can place rails or curated lists onto Home; ties into §16 ranking and A/B hooks.
11. **Analytics:** Page views, module CTRs, KB search/zero results, helpfulness votes tracked.

## 9.12 QA checklist (tie to §22)

* Author→Editor workflow: draft → in\_review → published; notifications fired.
* Legal doc: two‑person publish; version history; effective date banner; prior versions accessible.
* Preview tokens: expire correctly; render exact content; noindex.
* Home: modules render; Discovery rail pulls correct items; Lighthouse budgets green.
* Contact form: validation, CAPTCHA, rate limit; ticket created; autoresponder.
* KB: search with synonyms; article ToC anchors; helpfulness voting stores results; related links correct.
* Redirects: 301/302 created; conflict detection works; bulk import from CSV.
* Menus: edit & reorder; broken link warnings; header/footer reflect changes.
* OG images: auto generator preview; custom upload size validated; sharing cards show properly (Facebook/X/LinkedIn).
* Security: script injection attempt stripped; broken embed shows safe fallback.
* Sitemaps/robots: validate; zero‑result pages not indexed; 410 for archived pages.
* A11y: keyboard traverse header/footer; accordion FAQ; alt text required; color contrasts pass.

## 9.13 Microcopy kit (marketing)

* **Contact form success:** “Thanks! We’ve received your message and will get back to you soon.”
* **KB helpfulness:** “Was this article helpful?” “Yes” / “Not really” / “Tell us more (optional)”.
* **Preview banner:** “Preview — visible only to people with this link.”
* **Legal effective date:** “Effective **{date}**. Prior versions: {dropdown}.”
* **OG image missing:** “For best results, upload a 1200×630 image.”

## 9.14 Optional add‑ons (Phase‑2)

* **Blog / News** content type with author bios and RSS.
* **Email capture (double opt‑in)** module for marketing (kept off by default per §6 consent).
* **Localization** (i18n) with per‑page language variants and hreflang.
* **A/B testing framework** for module order & copy variations (ties to §20.Q).
* **Link checker** nightly job (broken internal/external links report).
* **Content quality lints** (Flesch reading grade, passive voice, long sentences).

## 9.15 Implementation notes

* Prefer a **headless CMS** (self‑hosted or managed) with webhook on publish → triggers **edge cache purge** and (optionally) **static regeneration** of affected routes.
* Maintain a **content registry** service mapping CMS IDs to routes for quick invalidation.
* All content rendered with **SSR sanitization** and **component mappings** from modules → React/Vue components (or your framework equivalents) that implement §4 standards.

# Section 10 — User Portal

## 10.0 Overview

**Scope:** Portal IA, Profile & Security, Wallet, Payments, Donations, Rewards, Teams, Messaging (DM), Share, Support, Verification, Preferences, Public Entity Profiles, accessibility, performance, privacy toggles.  
**Depends on:** Sections 0 (policies), 3 (roles/COI), 11 (KYC), 12 (team & rewards), 14 (checkout), 15 (payouts), 18 (notifications), 20 (Admin & moderation).

## 10.A Navigation & IA (your structure, expanded)

**Top‑level portal nav (left rail):**

* **Profile (Home)**  
  ▸ **Edit Profile**  
  ▸ **Security** (alias/shortcut also shown at top level)  
  ▸ **Settings** (privacy, visibility, messaging rules)  
  ▸ **Verification**  
  ▸ **Payments** (saved payment methods for donations)
* **Security** (shortcut to the same Security page)
* **Wallet** (organizers; balance, payouts, tax center)
* **Donations**
* **Rewards**
* **Teams** (visible if Lead/Co‑Lead/Member/Support)
* **Messaging** (Direct Messages inbox with portal notifications)
* **Share** (Share & Referrals hub across campaigns/teams)
* **Support** (tickets, KB)

**Navigation rules & AC**

* **AC‑IA‑1:** Breadcrumbs reflect sub‑pages; back to top of section within two clicks.
* **AC‑IA‑2:** Role‑aware: items hidden if not applicable (e.g., Wallet visible only if organizer has/ had a campaign).
* **AC‑IA‑3:** Mobile: collapsible left rail; persistent bottom “Inbox” and “Support” shortcuts.

**Login landing (10.A.2)**

* If user is an organizer with any live/ended campaigns → **Organizer Dashboard card** at top of **Profile (Home)** showing active campaigns and quick KPIs; otherwise land on **Donations** overview. (You selected default.)

## 10.B Profile & Identity

**10.B.1 Edit Profile (defaults)**

* Fields: Username (read‑only), First/Last, Email, Phone, Website, Company/Business, DOB, Address (street/city/state/zip; **Address Book** with Default shipping/Default billing), Avatar (cropper).
* **Addresses autocompletion:** USPS/Smarty enabled.

**Flows & AC**

* **Email change:** confirm via link to **current email**, then set **new email**; new email must be verified before becoming primary.
* **Phone change:** **SMS OTP** to new number before save.
* **AC‑PRO‑1:** Username immutable post‑registration.
* **AC‑PRO‑2:** Address Book supports add/edit/delete; one default per type.

**10.B.2 Linked Accounts**

* Apple/Google sign‑in link/unlink (requires password to unlink). (Default)

## 10.C Security (you chose defaults + extras)

* **2FA:** Authenticator app (TOTP) + SMS fallback; show Recovery codes once (download & copy).
* **Active sessions/devices:** device, last active, approximate location; “Sign out of all other sessions.”
* **Security log:** last 50 events (login, password change, 2FA changes, device revocations).
* **Account deletion:** Request → 14‑day cooling; blocked if outstanding rewards, open disputes, negative balance, or pending payouts. Option to anonymize public donor display where policy allows.

**AC**

* **AC‑SEC‑1:** “Sign out all” invalidates tokens within 30 seconds.
* **AC‑SEC‑2:** Deletion request shows a checklist of blockers, with links to resolve.

## 10.D Wallet (organizers)

* **Balance:** Eligible, On Hold, Reserved, Net Available, Next Payout ETA (mirrors Section 15).
* **Payout History:** table + filter; statement **PDF/CSV** downloads.
* **Payout Destination:** Stripe‑hosted flow; OTP + **24h cooldown** after change; name mismatch prompts review (Section 15).

**AC**

* **AC‑WAL‑1:** Cooldown blocks “Request Payout” until timer elapses.
* **AC‑WAL‑2:** Statements reflect config (cover fees mode) and match Finance statement.

## 10.E Payments (donors’ saved methods)

* Cards via Stripe, Apple Pay, Google Pay, Stripe Link. Set default; add/edit/remove.
* Billing address optional (only if required by processor).
* Network Account Updater enabled for expired cards.

**AC**

* **AC‑PM‑1:** Removing the default card prompts to set another as default first.
* **AC‑PM‑2:** PCI copy displayed; sensitive fields hosted by Stripe.

## 10.F Donations (History & Receipts)

* **List view:** filters (date range, campaign, status: Success/Refunded/AoN‑Refunded), amount min/max; search by campaign title.
* **Detail view:** receipt breakdown (donation/tip/fees/net), AoN label, PDF receipt, team attribution (if any), reward status link, **Request refund** button.
* **Export:** CSV of own donations.

**AC**

* **AC‑DON‑1:** Refund request opens a modal (reason, notes) and creates a ticket (Section 20).
* **AC‑DON‑2:** AoN auto‑refund shows clear badge and net $0.

## 10.G Rewards (donors)

* **Rewards list:** Campaign, Tier, Status (Unfulfilled/Pending/Processed), Last update, Actions.
* **Detail:** organizer notes (if shared), tracking link, ability to **update shipping** until status becomes **Pending**; **gift digital reward** to another email (before Pending).

**AC**

* **AC‑RWD‑1:** Portal banner persists for unclaimed eligible rewards until claimed/opted‑out.
* **AC‑RWD‑2:** All edits audit‑logged (who/when/from→to).

## 10.H Verification (hub)

* Tiles: Email, Phone, **ID (DL/State)**, **SSN last‑4**; **EIN** tile appears if switching to org account.
* DL upload UX with capture guidance; **manual review** fallback with ETA.
* Verified users display **gold star badge** on avatar (tooltip text set in copy kit).

**AC**

* **AC‑VER‑1:** Campaign cannot publish unless 4/4 verified (Section 12.O gate).
* **AC‑VER‑2:** EIN required for organizations/charities prior to payout.

## 10.I Teams (end‑user view)

* Shows the Team module pages from **Section 12.J** if the user is Lead/Co‑Lead/Member/Support. (Default)

## 10.J Share (Share & Referrals hub)

* Aggregates **Team** and **Member** links across all live campaigns; quick copy buttons; QR downloads.
* Mini‑metrics: clicks, donations, amounts by campaign & by member (if applicable).
* Social presets (FB, X/Twitter, LinkedIn, email) with editable share text.

**AC**

* **AC‑SHARE‑1:** Member sees only their metrics; Organizer sees all.
* **AC‑SHARE‑2:** QR images download as PNG; links include correct ref= and UTM.

## 10.K Notifications & Preferences

* **Channels:** Email & SMS per family (Donations, Rewards, Payouts, Team, Verification, Security). Some events are mandatory (security, legal).
* **Quiet hours:** SMS snooze window (default 9pm–8am local), with security exceptions.
* **Digests (decision):** **Keep optional, default OFF** for all users (organizers can enable weekly digests once they have a live campaign).
* **Marketing:** opt‑in only (unchecked).

**AC**

* **AC‑NOTIF‑1:** Changing a channel shows effective events; mandatory items can’t be disabled.
* **AC‑NOTIF‑2:** Quiet hours never delay security notices.

## 10.L Support & Help

* **Support:** Submit ticket (category, subject, details, attachments), ticket history; KB quick links. (Default)
* **Report a problem:** persistent “?” icon routes to Support with context. (Default)

## 10.M Accessibility & UX (defaults)

* WCAG 2.2 AA: keyboard navigation, visible focus, live regions for validation; avatar cropper keyboard support.
* Inline validation with examples.

## 10.N Empty states & education

* Friendly starter panels (no campaigns/donations/rewards yet) with CTAs to start/browse. (Default)

## 10.O Edge cases & guardrails

* **Email change with 2FA:** require password + 2FA; warn about recovery codes.
* **Phone change:** locks payout request for **24h** (cooldown).
* **Deleting default card:** must choose another default first.
* **Default donor preference:** allow user to set preferred **“Hide my name publicly”** (pre‑checked in checkout). **Anonymous** remains a per‑donation choice.

**AC**

* **AC‑EDGE‑1:** Checkout respects the user’s default hide‑name preference but never auto‑selects Anonymous.
* **AC‑EDGE‑2:** Cooldown banners link back to Wallet or Security as appropriate.

## 10.P Copy & tone

* Warm/helpful, concise; tooltips for AoN, fees, anonymity.

## 10.Q Data & Exports

* **Download my data** (GDPR‑style) triggers DSAR workflow (Section 20.U). (Default)

## 10.R Performance targets

* TTI on 4G: Profile < **1.0s**, Donations list < **1.5s**, Rewards < **1.5s**, Wallet panels < **1.2s**. (Default)

## 10.S Messaging (Direct Messages) — ****NEW****

**Purpose:** Privacy‑protected in‑portal messaging between registered users and organizers (and for reward fulfillment), with portal notifications and email/SMS alerts per preferences.

### 10.S.1 IA & Entry points

* Top‑level **Messaging** item shows **Inbox** (default), **Sent**, **Archived**, **Blocked**.
* Compose from:
  + **Entity profile pages** (User/Org/Team) via “Message” button.
  + **Rewards detail** (“Contact organizer”)—routes into the same inbox thread.
  + **Campaign page** (optional Phase‑2: “Message organizer” if organizer allows).

**AC**

* **AC‑MSG‑1:** If recipient has disabled DMs, “Message” shows disabled with tooltip: “This user isn’t accepting messages.”

### 10.S.2 Thread model & features

* One thread per **sender×recipient** pair per **context** (general vs reward).
* Rich text (bold/italic, links), no images in MVP.
* Attachments for **Rewards context only** (e.g., proof/tracking) — files ≤ 5 MB; types: pdf/jpg/png.
* Read receipts (“Seen”), typing indicator (optional Phase‑2).
* Mark unread, star, archive.
* Search messages by keyword and recipient.

**AC**

* **AC‑MSG‑2:** Messages are private; email addresses not exposed.
* **AC‑MSG‑3:** Attachments are virus‑scanned; blocked types rejected with clear error.

### 10.S.3 Notifications & rules

* New message: portal badge + email; SMS optional (respects quiet hours).
* Mute conversation: stops email/SMS for that thread.
* Auto‑throttle: max **5 new conversations/day** per user; **30 messages/hour** to prevent spam (configurable).

**AC**

* **AC‑MSG‑4:** Abuse controls: **Report** message; **Block** sender; blocked users cannot start new threads.

### 10.S.4 Privacy & moderation

* Organizer can **restrict who can message them**: Anyone (default), Donors‑only, No one.
* Donor can block any user.
* Reported messages create **Moderation cases** (Section 20.B) with the message snapshot.

**AC**

* **AC‑MSG‑5:** If “Donors‑only,” compose checks whether sender donated to any campaign by that organizer.

### 10.S.5 Data model (additions)

* **MessageThread**(id, context: general|reward, subject, created\_at, last\_msg\_at)
* **MessageParticipant**(thread\_id, user\_id, role: sender|recipient, muted, blocked, archived)
* **Message**(id, thread\_id, sender\_id, body\_html, attachment\_ref, created\_at, seen\_at)
* **MessageReport**(id, message\_id, reporter\_id, reason, created\_at, moderation\_case\_id)

## 10.T Public Entity Profiles (User / Organization / Team)

**Goal:** Make profile/organization/team names clickable across the site, leading to a **public profile page** with optional stats and a “Message” CTA.

### 10.T.1 Where names are clickable

* Campaign headers (organizer name), team leaderboard (member names), donation lists (respecting privacy rules), updates, comments (when launched), search result cards, Support replies.  
  **Privacy:**
* **Anonymous donors**: never clickable, display “Anonymous”.
* **Hide‑name donors**: public name hidden, but organizer still sees contact for rewards; no public link.

**AC**

* **AC‑PUB‑1:** All clickable names route to the correct entity type: /u/{username}, /org/{org\_slug}, /team/{campaign\_slug} (configurable slugs).

### 10.T.2 Public profile content (by entity type)

**User profile (/u/{username})**

* Header: avatar (+ gold star if verified), display name, **Member since {date}**, city/state (optional), “Message” button.
* **Campaigns**: Current (live), Past (ended).
* **Stats panel (optional; user can hide in Settings):**
  + **Total raised** across campaigns created
  + **Donated totals**: last **7 days**, **30 days**, **6 months**, **1 year** (successful donations only; excludes refunds/AoN auto‑refunds)
  + **Largest donation made** (amount + link to campaign if visible)
  + **Largest donation received** on one of their campaigns (amount + link)
* Social links/website (optional).

**Organization profile (/org/{org\_slug})**

* Header: org logo, verified badge (if EIN verified), location, “Message” button.
* Org description (admin‑managed), link to website.
* Campaigns grid (current & past).
* **Stats panel (optional, hideable by Org Admin):** total raised across org campaigns, same donor/time breakdown if desired (org‑wide).

**Team profile (/team/{campaign\_slug})**

* Campaign title + cover thumbnail, team photo/description, leaderboard (if enabled), “Message Team” (routes to Team Lead inbox).
* Team members with amount raised (names clickable to user profiles if allowed).

**AC**

* **AC‑PUB‑2:** Stats visibility toggles live in **Profile → Settings** and **Org Admin → Settings**; default **ON for raised**, **OFF for donations‑made** to respect privacy.
* **AC‑PUB‑3:** Stats calculate from successful donations only (exclude refunds & AoN not funded).
* **AC‑PUB‑4:** “Message” obeys the recipient’s DM preferences (Anyone / Donors‑only / Off).
* **AC‑PUB‑5:** If a user hides all stats, the panel is omitted (no empty shell).

### 10.T.3 Settings controls (new toggles)

**Profile → Settings → Privacy & Visibility**

* “Show **Total raised** across my campaigns” (ON by default)
* “Show **My donations made** totals on my public profile” (OFF by default)
* “Show **Largest donation made**” (OFF by default)
* “Show **Largest donation received**” (ON by default)
* “Allow direct messages from: Anyone / Donors‑only / No one” (default: **Anyone**)
* “Allow organization/team pages to list me as a member” (ON; if OFF, shows “Name hidden” to the public team list but still functional for attribution)

**AC**

* **AC‑SET‑1:** Changing these toggles updates public pages immediately and writes to AuditLog (what changed, by whom, when).
* **AC‑SET‑2:** “Name hidden on team page” does **not** reduce attribution for referrals.

### 10.T.4 SEO & share

* Each profile gets a share card (OG image) with avatar/logo, display name, and (if enabled) a stat like “Raised $X so far”.
* Canonical URLs and slugs editable by Admin (Section 20.P).
* Optional “Follow” (subscribe to organizer updates) can be Phase‑2.

## 10.U Organizer Dashboard (Profile Home enhancements)

When the user has any live/ended campaigns, **Profile (Home)** shows:

* Cards for active campaigns (raised/goal, days left, quick links to Team, Rewards, Share).
* **Tasks panel** (coach cards): Add cover image, Post an update, Invite teammate, Finish verification. (You accepted this MVP feature.)

**AC**

* **AC‑DASH‑1:** Tasks disappear automatically when completed.

## 10.V Acceptance Criteria (summary)

* **IA:** Your menu structure implemented; role‑aware visibility; mobile‑friendly.
* **Profile & Security:** Email/phone flows, address book, TOTP/SMS 2FA, session/device list, security log, deletion cooling period.
* **Wallet & Payments:** Mirrors payouts spec; card vault via Stripe; NAU updates.
* **Donations & Rewards:** Filters, receipts, reward claim edits; persistent banners.
* **Verification:** 4/4 gate; EIN for orgs.
* **Teams & Share:** Integrates Section 12.J; member‑only metrics; UTM/ref links correct.
* **Notifications:** Per‑family toggles; Quiet hours; digests optional OFF.
* **Support:** Ticketing + KB; context pass‑through.
* **Messaging:** Inbox + DM from public profiles; abuse controls; rate limits; attachments in reward context only; report/block.
* **Public Profiles:** Clickable names site‑wide; user/org/team pages; optional stats; DM CTA; privacy toggles.
* **Accessibility:** WCAG 2.2 AA controls; inline validation; keyboardable cropper.
* **Performance:** TTI targets met.

## 10.W Data Model (conceptual deltas)

* **UserProfile**: username, display\_name, avatar\_ref, city, state, **privacy\_settings** (booleans above), **dm\_policy** (anyone|donors|off), joined\_at.
* **OrgProfile**: org\_slug, name, logo\_ref, description, url, privacy\_settings, dm\_policy.
* **TeamProfile**: campaign\_id, photo\_ref, description, leaderboard\_enabled.
* **ProfileStatsCache**: entity\_type (user|org|team), entity\_id, totals (raised\_all\_time, donated\_7d/30d/6m/1y, largest\_donation\_made, largest\_donation\_received), computed\_at.
* **MessageThread, MessageParticipant, Message, MessageReport** (see 10.S.5).
* **AddressBook**: user\_id, type (shipping|billing), is\_default, address fields.
* **SecurityLog**: user\_id, event\_type, ip, device, ts.

## 10.X Microcopy (ready to ship)

* **DM disabled tooltip:** “This user isn’t accepting messages.”
* **DM abuse report:** “We’ve received your report. Our team will review.”
* **Public profile stats toggle off:** “This user prefers to keep these stats private.”
* **Default hide name (checkout hint):** “Your name will be hidden publicly. The organizer can still contact you for rewards.”
* **Organizer dashboard tasks:** “Invite a teammate to boost your reach.”

## 10.Y Open Configs (Admin‑editable via Section 20)

* DM rate limits; file types & size caps; profile stats defaults; quiet‑hours defaults; visibility default toggles; profile slug rules; address autocomplete provider keys.

# 

# Section 11 — Identity & Verification (KYC/KYB)

**Scope:** User & organization identity verification to **publish** campaigns and **payout** funds; risk‑based step‑ups; admin controls; privacy & retention; notifications; acceptance criteria; data model.  
**Vendors:** **Stripe Identity** (DL/State ID, optional selfie) + **Stripe Connect (Express)** (SSN last‑4, EIN, bank account onboarding).  
**Add‑ons included:** **Verified Nonprofit badge** (IRS check), **Weekly sanctions re‑screening**, **SIM‑swap risk check (Phase‑2)**.

## 11.0 Requirements recap

* **US‑only**, **18+** required.
* **Publish gate**: Email, Phone, **DL/State ID** (passed).
* **Payout gate**: **SSN last‑4 (individual)** OR **EIN (organization)** + **US bank** verified.
* **Gold star** on avatar when the four checks are green (email/phone/ID/SSN‑or‑EIN).
* Team roles: Only **Team Lead/Organizer** must complete full verification (Co‑Lead/Member/Support not required for KYC, but must have verified email/phone).

## 11.1 User flows (end‑to‑end)

### A) Publish gate (Organizer)

1. **Verification Hub** (Portal → Profile → Verification): tiles for **Email**, **Phone**, **ID**, **SSN/EIN** (Bank appears after SSN/EIN).
2. Organizer clicks **“Verify ID”** → **Stripe Identity** hosted flow (front + back of DL/State ID; selfie only if risk‑flagged).
3. Success → **ID: Verified**; failure → retry up to **3 attempts/24h**; then **Compliance Review** opens automatically.

**AC-PUB-1**: “Publish” button remains disabled until Email + Phone + ID are **Verified**.  
**AC-PUB-2**: If selfie step‑up triggered and skipped, mark **ID = Incomplete** and show “Resume verification” CTA.

### B) Payout gate (Organizer)

1. **SSN last‑4** (individuals) **OR** **EIN** + business profile (orgs) via **Stripe Connect** onboarding link.
2. **Bank account** added in the same hosted flow.
3. Name mismatch or EIN mismatch → **Compliance Hold** (payouts blocked) + request documentation (DBA, IRS letter, bank letter).

**AC-PO-1**: Payout request disabled until SSN/EIN and Bank are **Verified**.  
**AC-PO-2**: Name mismatch sets **Compliance Hold** with organizer‑facing banner and “Upload documents” CTA.

## 11.2 Accepted documents & capture rules

* **Accepted**: US Driver’s License, US State ID. (US Passport = Phase‑2 fallback)
* **Image rules**: front + back; glare/blur detection; auto‑crop; barcode/OCR validation.
* **Retry policy**: up to **3 attempts** per **rolling 24h**; thereafter route to **Compliance Review**.

**AC-DOC-1**: Failed capture presents actionable tips (lighting, glare, edges visible).  
**AC-DOC-2**: Expired ID → block; show guidance to upload a valid ID.

## 11.3 SSN (individuals) & EIN (organizations)

* **SSN**: **last‑4 only** (via Connect); matched against legal name/DOB from ID.
* **EIN**: via **Connect** business profile + authorized representative attestation; optional IRS letter upload if mismatch.
* **UBO data**: collected by Stripe if required (we store statuses only).
* **Outcome statuses**: verified | failed | manual\_review | info\_requested.

**AC-SSN-1**: We **never** store raw SSN; only token/status.  
**AC-EIN-1**: Verified orgs show **“Verified Organization”** badge on public org profile.

## 11.4 Address & age checks

* **Age ≥ 18** enforced from ID DOB.
* **Address**: US address only; USPS/Smarty autocomplete; editable during KYC; no utility bill at MVP unless Compliance requests.

**AC-AGE-1**: Under‑18 → publish/payout blocked; show guidance.  
**AC-ADDR-1**: Non‑US addresses blocked with friendly copy.

## 11.5 Name mismatch & bank verification

* **Bank name ≠ ID/legal name** → **Compliance Hold** (payouts blocked) until documentation supplied (DBA certificate, bank letter).
* **Cooldown**: Changing payout destination enforces **24h** security cooldown (Section 15).

**AC-NM-1**: Hold reason and requested documents displayed in Wallet → Payout Destination and in Verification Hub.

## 11.6 Attempt limits, cooldowns, re‑verification

* **ID attempts**: 3 per 24h; **SSN**: 2 per 24h; **EIN**: 2 per 24h (Connect).
* **Cooldown**: 24h after max attempts; contact Support for urgent cases.
* **Re‑verification**:
  + When name or DOB changes;
  + On suspicious activity;
  + **Sanctions re‑screening (weekly)** automatically (add‑on); ID re‑capture only if required.

**AC-LIMIT-1**: Attempt counters reset on rolling basis; hub shows “Try again in {hh:mm}”.

## 11.7 Risk‑based step‑ups (selfie / liveness)

**Triggers** (any): high‑risk IP/device (VPN/proxy, geolocation anomaly), repeated OCR mismatches, **large payout ≥ $50k** upcoming, or auto‑risk score high.  
**Action**: require **selfie/face match** via Stripe Identity before publish or payout (whichever occurs first).

**AC-RISK-1**: If triggered, hub tile indicates **“Selfie required”** and flow cannot be skipped.  
**AC-RISK-2**: Passing selfie clears the step‑up for 12 months (unless new risk event).

## 11.8 UX & accessibility

* **Verification Hub UI**: tiles show **status chip** (Green=Verified, Amber=Action required, Gray=Not started), **“Estimated time: ~2–3 minutes”**, and contextual CTAs.
* **Failure feedback**: plain language (“Retake in brighter lighting; make sure all corners are visible”).
* **Accessibility**: high contrast, keyboardable, screen‑reader hints; large click targets.

**AC-UX-1**: All flows meet **WCAG 2.2 AA**; transcripts for guidance videos when added.

## 11.9 Notifications

**Organizer**: ID verified/failed, SSN/EIN verified/failed, KYC under review, hold placed/released, weekly reminder if verification incomplete and a draft campaign exists.  
**Admin/Compliance**: new manual review case, SLA approaching, large payout requires selfie.

**AC-NOTIF-1**: All notices logged (Section 20); email + in‑app; SMS only for critical blockers if enabled.

## 11.10 Admin & Compliance Console (tie‑in to Section 20)

* **Queues**: KYC reviews, Name mismatches, EIN mismatches, Holds (Publish/Payout) with SLA timers.
* **Actions**: place/release **Publish Hold**, **Compliance Hold**, set **Reserve %**, **Request more info**, **Override** with reason (audited).
* **Doc viewing**: **Stripe‑hosted** only; no raw images stored or downloadable.
* **Audit**: actor, action, reason, timestamp; immutable.

**AC-ADMIN-1**: Overrides require step‑up and reason; dual‑approval optional for critical overrides.

## 11.11 Privacy & retention

* PII storage = **tokens & statuses only**; no raw SSN/ID images stored on our servers.
* Retain statuses, outcomes, and audit logs for **24 months** (policy‑configurable); purge per DSAR unless on legal hold.
* Public display shows **badges only**, never PII.

**AC-PRIV-1**: DSAR actions route to Admin (Section 20.U) and are auditable.

## 11.12 Edge cases

* **No smartphone/camera**: desktop upload supported by Stripe; else Support fallback.
* **Good‑faith mismatch**: provide “Explain discrepancy” text box + doc upload; Compliance reviews.
* **Team roles**: Co‑Lead/Member/Support do not need full KYC; organizer alone must pass to publish/payout.
* **Multiple campaigns**: KYC is **per organizer** (not per campaign); once verified, applies to all campaigns for that user (subject to re‑screen).

## 11.13 add‑ons (implemented)

### A) ****Verified Nonprofit badge**** (Org KYB enhancement)

* **Source**: IRS **Pub 78** / **BMF** cross‑check (via IRS data or trusted aggregator).
* **Flow**: On EIN verification, auto‑match legal name + EIN; if match, apply **“Verified Nonprofit”** badge on org profile & campaign headers; if mismatch, show **“Unable to confirm nonprofit status”** (non‑blocking) and open **Compliance Review**.
* **Refresh**: re‑check monthly (cache & version).  
  **AC-NP-1**: Badge only when EIN present **and** IRS match true.

### B) ****Weekly sanctions re‑screening**** (continuous KYC)

* **Scope**: All Verified organizers and org reps re‑screened weekly against sanctions lists (via Stripe/partner).
* **Outcome**: positive match → **Compliance Hold** + notify; negative → silent pass.  
  **AC-SCR-1**: Re‑screen log visible to Compliance with last‑screen date.

### C) ****SIM‑swap / phone risk**** (Phase‑2)

* **Trigger**: SMS OTP failures, sudden phone number change, high‑value payout.
* **Action**: require extra step‑up (email link + TOTP) or selfie if coupled with other risks.

## 11.14 Copy kit

* **Hub header**: “Verify your identity to launch your campaign and receive payouts.”
* **ID success**: “All set—your ID is verified.”
* **ID failure (retry)**: “We couldn’t verify your ID. Try again in good lighting and include all four corners.”
* **Selfie required**: “A quick selfie is required to complete verification.”
* **SSN/EIN tile**: “Provide your SSN (last 4) or EIN to enable payouts.”
* **Name mismatch hold**: “Your payout is paused while we confirm your payout details. Upload a DBA or bank letter to proceed.”
* **Verified Nonprofit**: “Status confirmed with IRS records.”

## 11.15 Data model (conceptual additions)

* **KycProfile**: user\_id, email\_verified, phone\_verified, id\_status {unstarted|verified|failed|manual\_review|selfie\_required}, id\_attempts\_24h, dob, age\_verified, last\_selfie\_at.
* **KybProfile**: org\_id, ein\_status {unstarted|verified|failed|manual\_review}, nonprofit\_status {unconfirmed|verified|failed}, irs\_last\_checked\_at.
* **PayoutEligibility**: user\_id|org\_id, bank\_status {unstarted|verified|mismatch}, compliance\_hold {none|publish|payout|reserve}, reserve\_pct, cooldown\_until.
* **VerificationAttempt**: id, user\_id, type {id|selfie|ssn|ein}, provider\_ref, status, error\_code, created\_at.
* **ComplianceCase**: id, type {name\_mismatch|ein\_mismatch|sanctions\_hit}, status, requested\_docs[], notes, opened\_at, closed\_at.
* **SanctionsScreening**: entity\_type {user|org}, entity\_id, screened\_at, result {clear|match|inconclusive}, provider\_ref.
* **Badges**: entity\_type, entity\_id, badge\_key {verified\_user|verified\_org|verified\_nonprofit}, granted\_at, revoked\_at.

## 11.16 Acceptance Criteria (summary)

* **Publish gate** blocks until **Email + Phone + ID** verified, with clear CTAs in Hub.
* **Payout gate** blocks until **SSN or EIN + Bank** verified; name mismatch → **Compliance Hold** with guidance.
* **Risk step‑ups** trigger and enforce selfie/liveness where needed; passing unlocks flow.
* **Limits & cooldowns**: attempts enforced; cooldown timers shown; Support path exists.
* **Weekly re‑screen** runs and logs results; positive matches place **Compliance Hold**.
* **Verified Nonprofit badge** appears on org profile/campaign only after IRS match.
* **Privacy**: no raw SSN/ID stored; statuses only; DSAR supported.
* **Accessibility**: flows meet WCAG 2.2 AA.
* **Audit**: all state changes and overrides recorded with actor, reason, timestamp.

# 

# Section 12 — Campaign Creation & Rewards

**12.0 Overview**  
• **Scope:** Campaign creation wizard (steps, fields, validations, copy), visuals and media limits, reward tiers (optional), donor reward claiming, organizer fulfillment tooling, **team fundraising (roles, invites, referral attribution, leaderboard, support seats)**, public campaign page modules, notifications, analytics, edge cases.  
• **Dependencies:** Section 0 policies (KWR/AoN, deadlines, verification), Section 3 (roles/permissions + affiliation rules), Section 11 (KYC gate), Section 14 (checkout), Section 15 (payout timing), Section 18 (notifications).

## 12.A Campaign basics

### 12.A.1 Category taxonomy (proposed)

Primary categories (choose one at creation; optional tags unlimited):

1. Medical & Health
2. Memorial & Funerals
3. Emergency & Disaster Relief
4. Education & Learning
5. Community & Neighbors
6. Animals & Pets
7. Creative, Arts & Culture
8. Sports & Teams
9. Business & Entrepreneurship
10. Environment & Sustainability
11. Faith & Causes
12. Charities & Nonprofits  
    **Tags** (examples): surgery, funeral, wildfire, tuition, classroom, shelter, rescue, film, album, youth sports, startup, green, church, synagogue, grant, matching.

**AC**  
• **AC CAT 1:** Campaign must select exactly one category; can add 0–10 tags.  
• **AC CAT 2:** Disallowed categories cannot be selected (policy filter).

### 12.A.2 Goal & amounts

• Goal required. **Minimum $100** (recommended floor to avoid trivial campaigns); no maximum.  
• **Donation minimum:** $5; **no max** (subject to processor limits).

**AC**  
• **AC GOAL 1:** Goal ≥ $100; numeric; **whole dollars only** for MVP.  
• **AC GOAL 2:** Donation control enforces ≥ $5.

### 12.A.3 Location

• Display **city & state** on campaign.  
• Input source: organizer’s profile address prefill; editable to a city/state selector.

**AC**  
• **AC LOC 1:** City/State required; **US only**.

### 12.A.4 Team fundraising (MVP)

• **Max 5 seats total** (including **Team Lead** + optional **Co‑Lead** + **Members**).  
• **Roles:** Team Lead (owner), **Co‑Lead** (max 1), Members (up to 3 if a Co‑Lead exists; up to 4 if no Co‑Lead).  
• **Join flow:** Lead adds by email → system creates **single‑use invite** → invitee accepts.  
– Not registered: completes **phone OTP + email verify**, sets password, joins.  
– Registered: logs in and joins.  
• **Attribution:** each member has a **unique referral link**; donations via that link credit **member** and **campaign**.  
• **Payout:** **one payout** to the campaign (no member‑level payouts).  
• **Leaderboard:** optional public module; shows member names & amount raised.

**AC**  
• **AC TEAM 1:** Cannot exceed **5 seats** (including Lead); UI blocks additional invites.  
• **AC TEAM 2:** Removing a member preserves historical attribution but **removes from leaderboard**.  
• **AC TEAM 3:** Lead can promote a Member to Co‑Lead; only **one Co‑Lead** allowed.

## 12.B Story & content

### 12.B.1 Rich‑text editor (decision made)

• Allow: **H2–H4**, bold/italic, lists, links, blockquote, **(Phase‑2: inline images)**.  
• Disallow: scripts/iframes (except vetted video embeds), form elements.  
• Auto‑sanitize HTML; strip tracking params from links.

**AC**  
• **AC RTE 1:** Soft limit **20,000** chars (warn at 90%); hard cap **30,000**.  
• **AC RTE 2:** Links https‑only; new tab; rel="nofollow noopener".

### 12.B.2 FAQ

• No hard policy limit; UI supports **up to ~50** items.  
• Links allowed; sanitized like story.

**AC**  
• **AC FAQ 1:** Add, edit, reorder, delete; collapsible on public page.

### 12.B.3 Organizer Updates (decision made)

• Enabled MVP (simple).  
– Content: text + **one image** per update.  
– Rate limit: **max 1/day**.  
– Triggers donor notification opt‑in (email default).

**AC**  
• **AC UPD 1:** Newest‑first with timestamp; deletions logged.

## 12.C Visuals

### 12.C.1 Images

• Cover aspect **16:9**; **min 1600×900** (rec 1920×1080).  
• Types: **jpg, jpeg, png, webp**.  
• Per‑file ≤ **5 MB**; up to **15** images.  
• **Alt text required** for accessibility.

### 12.C.2 Videos

• Upload: **mp4, mov**; ≤ **100 MB**; up to **5**.  
• Embeds: **YouTube/Vimeo** via oEmbed (thumb generated).  
• **Autoplay off**; click‑to‑play.

### 12.C.3 Gallery behavior

• Public page uses a **carousel** (images + videos).  
• Upload includes **crop/positioning** tool.

**AC**  
• **AC VIS 1:** Enforce file limits; per‑item errors; show remaining quota.  
• **AC VIS 2:** **Cover image required** to publish.

## 12.D Reward tiers (optional)

### 12.D.1 Tier model (rules)

• Up to **6 tiers**; **strictly ascending** (Tier N > Tier N‑1).  
• Organizer **may skip** rewards entirely.  
• **Per donation** eligibility (MVP): one donation qualifies for **one** tier (the **highest** met). No combining multiple donations in MVP.  
• **AoN:** do not fulfill rewards until **goal met**.

### 12.D.2 Per‑tier fields

• Amount (USD)  
• Tier name (e.g., “Signed Book”)  
• Description (rich‑text subset; links allowed)  
• **Estimated delivery date** (month & year)  
• **Delivery type**: Physical or Digital  
• **Quantity limit** (optional; 0 = unlimited)  
• **Options** (key/values, e.g., Size: S/M/L)  
• **Shipping required** (yes/no; triggers address on claim)  
• **Shipping region**: US‑only (optional state exclusions)  
• **Organizer notes (private)** (visible in fulfillment only)

**AC**  
• **AC TIER 1:** Cannot save non‑ascending tiers.  
• **AC TIER 2:** When **Quantity limit** reached → show **“Sold out”**; disable tier in UI.

### 12.D.3 Donor reward claim flow

• After donation **≥ Tier 1**:  
– Reward Claim page: **Claim** (contact + shipping if Physical; options), **Opt out**, or **Donate anonymously** (no claim; organizer sees “anonymous”).  
• **Hide my name publicly** still allows reward claim (organizer gets contact).

**AC**  
• **AC CLAIM 1:** If donor abandons claim, show persistent portal banner **“Finish reward claim”** until completed/opted‑out.  
• **AC CLAIM 2:** Donor can **edit** shipping until organizer sets status **Pending**.

## 12.E Donation & checkout specifics

• Show pre‑payment **fee breakdown**: donation, optional tip, fees (if “cover fees” ON), **net to campaign**.  
• **Consent** checkbox required (ToS, Privacy, Community Guidelines).  
• **AoN banner** when applicable: “You will be charged now. If the goal isn’t met by {deadline}, you’ll be automatically refunded.”

**AC**  
• **AC CHK 1:** Block submission without consent.  
• **AC CHK 2:** For AoN, email receipt reiterates refund condition.

## 12.F Organizer reward fulfillment

### 12.F.1 Fulfillment table (Organizer portal)

**Columns:** Donor username • First/Last name • Donation amount • Donation date/time (local) • Tier level • Delivery type • Contact • Shipping address • Options • Tracking number • **Status:** Unfulfilled → Pending → Processed • Notes (organizer‑visible + optional donor‑visible).  
**Actions:** **Bulk status update**; add **tracking**; add **note** (“share with donor”).

**AC**  
• **AC FUL 1:** Status change triggers donor **portal + email + SMS** notification.  
• **AC FUL 2:** Status change **audited** (who/when/from→to).

### 12.F.2 Nudges (decision made)

• **14 days** post‑campaign end: “Unfulfilled” reminder.  
• **30 days:** second reminder.  
• **45 days:** escalate to Support; donors notified of delay.

## 12.G Public campaign page (MVP modules)

1. **Header:** cover, title, **verified badge** tooltip (“Verified: email, phone, ID”), organizer, city/state, category.
2. **Progress:** raised, goal, **days left**, KWR/AoN label.
3. **Donate widget:** amount chips + “Other”, tip control, **cover fees** toggle, Donate.
4. **Team leaderboard (optional):** members + amount raised.
5. **Gallery carousel**.
6. **Story**.
7. **FAQ**.
8. **Updates**.
9. **Social share** (Facebook, X/Twitter, LinkedIn; copy link).
10. **Report this campaign** (donors‑only).
11. **Recent donors & messages** (respects hide‑name & anonymous).

**AC**  
• **AC PAGE 1:** If organizer not fully verified (4/4) → **cannot publish**; wizard shows blocking banner (no public page).  
• **AC PAGE 2:** If AoN not funded at deadline → show **“Not funded – all donations refunded”**; Donate disabled.

## 12.H Policies & edge cases (finalized)

• Change **funding model** after launch: **Not allowed**.  
• Change **goal** after launch: **Allowed upward once**; never below amount raised; donors notified.  
• **Deadline extensions:** **KWR only**, one extension up to **14 days**, requested ≥48h before original deadline; **AoN cannot extend**.  
• **AoN & rewards:** No fulfillment before success; if **not funded** → claims void.  
• **Anonymous & rewards:** Fully anonymous donors **cannot** claim rewards; hidden‑name donors **can**.  
• **Quantity‑limited tiers:** show **Sold out** status; no overselling.  
• **Affiliation donation rule (COI):** Only the **Team Lead/Organizer** may donate to **their own** campaign (flagged); all other affiliated roles (Co‑Lead, Member, Campaign Support, Org Admin/Support) **blocked** from donating to that specific campaign. (Details in Sections 3 & 14.)

## 12.I Notifications (Email/SMS/Portal)

**Organizer**  
• New donation; Tier sold out (first time); Reward claim submitted/updated; Reward status updated (bulk/manual); Unfulfilled nudges 14/30/45 days; **Team:** member invited/joined/removed; role changed.

**Donor**  
• Donation receipt (AoN recap when applicable); Reward claim required/confirmed/updated; Reward status Pending/Processed; Tracking provided; AoN outcome (funded vs auto‑refund).

**Team members**  
• Invite received; joined; removed; role change; **referral link regenerated** (if applicable).

## 12.J Team module — Portal pages & permissions

### 12.J.1 Pages (Campaign → Team)

• **Overview**  
– Team snapshot (total raised; % of campaign; members; 7/28/90d switcher).  
– **Leaderboard** (if enabled): Rank • Member • Amount raised • Donations • Conversion %.  
– **Share & Boost (quick):** Copy **Team Link**, **My Link** (if viewer is member), social share, **QR code** (download PNG).  
– Nudges: “Invite teammates (seats left: X)”, “Post an update”.

**AC**  
– **AC TEAM OVR 1:** Leaderboard shows only **active** members.  
– **AC TEAM OVR 2:** Copy link & QR work for Team and **current member** contexts.

• **Members & Roles**  
– Seat counter: “Seats used: **{count}/5** (Lead + Co‑Lead + Members)”.  
– Table: Avatar • Name • Role • Joined • Last activity • Amount raised • Actions (**Promote/Demote**, **Remove**).  
– Buttons: **Add Member**, **Add Co‑Lead** (disabled if one exists).  
– Side panel: **Campaign Support** summary (with link to Support tab).

**AC**  
– **AC TEAM MR 1:** Cannot exceed **5**; UI blocks invites over cap.  
– **AC TEAM MR 2:** Promote to Co‑Lead disabled if one already exists.  
– **AC TEAM MR 3:** Removing a member immediately revokes access and invalidates their referral link.

• **Member Details** (sub‑page)  
– Profile summary (role, joined, last activity).  
– **Referral link** (Lead/Co‑Lead can **regenerate**; Member sees read‑only).  
– Performance (visits, donations, amount; sparkline; timeframe).  
– Attribution list (read‑only, no donor PII).  
– Actions: Promote/Demote, Remove, **Regenerate link**.

**AC**  
– **AC TEAM MD 1:** Regenerating link **invalidates immediately**; audit entry written.  
– **AC TEAM MD 2:** Member self‑view cannot edit role or regenerate link.

• **Invites**  
– Table: Email • Role • Sent • Expires in • Status (Pending/Accepted/Revoked/Expired) • Actions (Resend, Revoke).  
– **Invite modal:** email, role (Member/Co‑Lead), seat cap validation, **conflict warning** (if invitee is Support on this campaign).

**AC**  
– **AC TEAM INV 1:** Invites are **single‑use**, **email‑bound**, **expire in 7 days**; **Resend** regenerates token & invalidates prior.  
– **AC TEAM INV 2:** Accepting a new role that conflicts (e.g., Support ↔ Member) **revokes** the older role in this campaign scope (with notifications).  
– **AC TEAM INV 3:** If invitee is logged in with a different email, show **Switch account** flow (cannot accept until emails match).

• **Settings**  
– **Leaderboard visibility** toggle.  
– Team photo & description (public).  
– **Ownership transfer**: Lead → **Verified** Co‑Lead (requires **SMS OTP**); Lead cannot leave until transfer completes.  
– **Leave team:** Co‑Lead/Member can leave; attribution remains.

**AC**  
– **AC TEAM SET 1:** Ownership transfer requires OTP; writes **AuditLog**; both parties notified.  
– **AC TEAM SET 2:** Leaderboard toggle updates public page instantly.

• **Share & Referrals**  
– Tabs: **Team Link**, **My Link**, **Channel presets** (FB/X/LinkedIn, Email), **QR code**.  
– **UTM** templates auto‑applied; **member code** param for attribution.  
– Mini‑analytics: Clicks, unique visitors, donations, amount (Team vs Me; 7/28/90d).

**AC**  
– **AC TEAM SHR 1:** Copy buttons & QR downloads work cross‑browser.  
– **AC TEAM SHR 2:** Members only see **their** metrics; Lead/Co‑Lead see **all**.

• **Support** (Campaign Support seats — separate from team seats)  
– Seats used: **0/2** (configurable).  
– Table: Name/Email • **Permissions** (checklist) • Assigned by • Added • Actions (Edit permissions, Remove).  
– **Invite Support**: email + optional permissions (**off by default**): View donor list; Export CSV; Moderate comments; Manage reward fulfillment.

**AC**  
– **AC TEAM SUP 1:** Support seats **do not count** toward team 5‑seat cap.  
– **AC TEAM SUP 2:** Campaign Support **cannot donate** to this campaign (COI); cannot publish/cash out.

### 12.J.2 Permissions (recap)

• **Team Lead:** manage campaign; publish/unpublish; manage rewards; invite/remove members; promote/demote; toggle leaderboard; edit team profile; request payout (outside Team tab).  
• **Co‑Lead:** everything Lead can do **except** delete campaign or transfer ownership/cash out.  
• **Member:** view team analytics; access **own** referral link; cannot edit rewards or campaign settings.  
• **Campaign Support:** scoped helper; by default can manage reward fulfillment & updates (if toggled), but **cannot** invite/publish/refund/payout; donation to this campaign **blocked** (COI).

**AC**  
• **AC TEAM UI 1:** Invite links are **single‑use**, **expire in 7 days**; can be **resent** (new token).  
• **AC TEAM UI 2:** Removing a member **revokes** their referral link; old links show **“invalid or expired.”**  
• **AC TEAM UI 3:** Role changes reflect **mid‑session**; sensitive downgrades trigger a secure refresh.

### 12.J.3 Referral & leaderboard attribution (logic)

• Attribution uses **member referral code** in session (ref=tm\_{member\_id}); **last‑touch** wins if multiple codes exist.  
• If a member is removed, historic attribution remains; member disappears from current leaderboard.  
• **Refunds** reduce totals; **AoN not funded** donations do **not** count.

**AC**  
• **AC TEAM ATTR 1:** Donation detail shows **“Attributed to {member}”** (Admin & Lead/Co‑Lead views; no donor PII).  
• **AC TEAM ATTR 2:** Regenerating a member link stops attribution from the **old** code immediately.

## 12.K Analytics & reporting (campaign/team)

**Organizer dashboard**  
• Donations over time (sparkline + daily table).  
• Average donation, unique donors.  
• Conversion (visits→donations).  
• Reward tier uptake (count & % per tier).  
• Refunds (count, $).  
• Geography by state.  
• Device (desktop/mobile).  
• **Team view:** amount per member; top referrers; clicks→donations per member (7/28/90d); CSV export.

**AC**  
• **AC ANL 1:** Export CSV for donations (respect donor privacy & anonymity) and reward status.

## 12.L Data model (conceptual additions/fields)

• **Campaign:** id, organizer\_id, category, tags[], title, short\_desc, story\_html, city, state, goal, start\_date, end\_date, funding\_model (KWR/AoN), team\_enabled (bool), leaderboard\_enabled (bool), status (draft/live/ended/not\_funded/suspended), cover\_image\_ref.  
• **CampaignUpdate:** campaign\_id, author\_user\_id, body, image\_ref, created\_at.  
• **CampaignMedia:** campaign\_id, type (image/video), file\_ref or embed\_url, order, alt\_text, size.  
• **TeamMember:** campaign\_id, user\_id, role (lead/co‑lead/member), joined\_at, removed\_at, **referral\_code**, **referral\_active (bool)**.  
• **TeamInvite:** campaign\_id, email, role, token, **expires\_at**, **accepted\_at**, **revoked\_at**, **status** (pending/accepted/expired/revoked).  
• **ReferralLink:** campaign\_id, member\_user\_id, code, url, active (bool).  
• **ReferralAttribution (derived/stored):** donation\_id, member\_user\_id, campaign\_id, channel, utm\_\*.  
• **RewardTier:** campaign\_id, tier\_number, amount\_min, name, desc\_html, delivery\_type, est\_delivery\_month, quantity\_limit, options\_schema, shipping\_required (bool), shipping\_region.  
• **Donation:** id, campaign\_id, donor\_id, amount, tip, fees, is\_anonymous, hide\_name\_publicly, **attribution\_member\_id (nullable)**, funding\_model\_snapshot, created\_at.  
• **RewardClaim:** donation\_id, tier\_id, status (Unfulfilled/Pending/Processed), contact, shipping\_address, options\_selected, tracking\_number, donor\_visible\_note, organizer\_private\_note, updated\_by.

## 12.M Copy kit (microcopy highlights)

• **Tier Sold Out:** “This reward tier is fully claimed.”  
• **Anonymous donation:** “Organizer will not receive your contact details. Rewards are unavailable for anonymous donations.”  
• **Hide name:** “Your name will be hidden publicly, but the organizer will receive your contact details for any rewards.”  
• **AoN checkout banner:** “Charged now; automatically refunded if the goal isn’t met by {date}.”  
• **Nudge 14d:** “Heads up — you still have rewards to fulfill. Donors are waiting.”  
• **Nudge 45d:** “We’ve alerted Support to help you finish fulfilling rewards.”  
• **Affiliation blocked (COI):** “You’re part of this campaign’s team. Only the campaign owner can donate here.”  
• **Owner self‑donation (flag):** “Heads up—donations by campaign owners are reviewed to protect campaign integrity.”  
• **Invite email subject:** “{Campaign} invited you to be **{Role}**”  
• **Invite expired:** “This invite has expired. Ask your Team Lead to resend it.”  
• **Link regenerate:** “Your old link will stop counting toward your totals.”

## 12.N Error states & edge cases

• **Tier ascending violation:** “Each tier must be priced higher than the previous one.”  
• **Quantity limit breach:** attempt beyond limit → prevent + error.  
• **Invite over capacity:** “Teams can have up to **5** members (including you). Remove someone before inviting another.”  
• **Co‑Lead already exists:** “Only one Co‑Lead is allowed.”  
• **Invite expired:** “Invite link expired.” (CTA: request resend)  
• **Invite email ≠ logged‑in email:** show **Switch account** modal; cannot accept until matching.  
• **Conflicting roles (Support vs Member):** warning + confirm; accepting **revokes** prior role in this campaign.  
• **Media over limits:** per‑file size, per‑campaign count/type errors with inline messages.  
• **Shipping change after Pending:** block edits; show “Contact the organizer to request changes.”  
• **AoN not funded:** Auto‑refunds issued; reward claims invalidated; campaign shows **Not Funded**.  
• **Referral link regenerated:** old link invalid; show “invalid or expired”.

## 12.O Publish gate & review step (added for quality)

**Step 4 — Review & Publish**  
• Summary: title, goal, funding model, dates, city/state, cover image, categories/tags, story word count, FAQ count, media counts, reward tiers summary, **team status**.  
• Pre‑publish checklist:  
– ✅ Verified (email, phone, DL/ID)  
– ✅ **SSN last‑4** (required before payout; not needed to publish KWR; AoN can publish without SSN, but payout blocked until SSN)  
– ✅ Cover image present  
– ✅ City/State set  
– ✅ Goal within bounds  
• **Publish** → campaign becomes **Live**.

**AC**  
• **AC PUB 1:** Publish disabled until all checklist items are green.

# 

# Section 13 — Campaign Public Page

**13.0 Scope**

End‑to‑end UX for a single campaign’s public page: layout, modules, donate widget, states (KWR/AoN, live/ended/suspended), team leaderboard, gallery, story, FAQ, updates, sharing, report flow (donors‑only), organizer card, accessibility/performance, analytics events, and acceptance criteria.

**13.1 Layout & breakpoints**

**A) Desktop (≥1024px)**

* **Left (content, 66%)**: Header band → Gallery → Story → FAQ → Updates → Related campaigns.
* **Right (sticky, 34%)**: **Donate widget** (sticky within viewport), Share box, Organizer card, Team leaderboard (if enabled).
* Max content width 1200px; 24px gutters.

**B) Tablet (768–1023px)**

* Donate widget becomes sticky below header but above content sections; two‑column collapses at 900px.

**C) Mobile (<768px)**

* Single column; **bottom sticky Donate bar** with amount entry CTA opens a full‑screen donate sheet.
* Gallery shows as swipeable carousel first; Share and Organizer appear after Donate module.

**AC‑LAY‑1:** Sticky donate never overlaps footer or obstructs content; focus order preserved for keyboard users.  
**AC‑LAY‑2:** CLS ≤ 0.1 after images and sticky elements load.

**13.2 Header band (top module)**

**Contents**

* **Title** (H1) — 1–2 line clamp.
* **Badges**: *Verified user* (gold star), *Verified organization*, *Verified nonprofit* (if EIN+IRS match). Tooltip text from Copy Kit.
* **Organizer line**: “by {Organizer Name}” (clickable to profile) • City, State • Category.
* **Progress chip**: $X raised of $Y, % funded, N donors, Days left (or Ended {date}).
* **Funding model chip**: **KWR** or **AoN** with tooltip:
  + AoN: “Charged now; auto‑refunded if goal isn’t met by {deadline}.”

**AC‑HDR‑1:** Organizer/Org names are clickable to public profiles (Section 10.T).  
**AC‑HDR‑2:** AoN chip appears only when funding\_model = AoN.

**13.3 Donate widget (sticky)**

**Fields & controls**

* **Quick amount chips** (configurable via Admin): e.g., $25 • $50 • $100 • $250 • Other.
* **Custom amount** input (whole dollars only; min $5).
* **Tip** control (default off/on per platform config; user editable).
* **Cover fees** toggle (if enabled).
* **Show impact** (optional note: “Your $50 helps pay for…” from organizer’s short text; optional).
* **Primary CTA:** **Donate** (routes into Checkout flow from Section 14).
* **Secondary actions:** Share, Copy link, QR.
* **Guardrail text**: shows min amount error; soft warning on unusually high amount (from 14.B.6); blocks below $5.

**State logic**

* **Affiliation rule** (COI, Section 3):
  + If viewer is **Team Lead** (owner) → allow donation but **flag** as self‑donation post‑checkout.
  + If viewer is **Co‑Lead/Member/Support/Org Admin for this campaign** → **block** with copy: “You’re part of this campaign’s team. Only the campaign owner can donate here.”
* **KYC gate**: Not relevant to donor; only organizer gates.
* **Suspended** / **Not funded (AoN)** / **Ended**: disable donate, show reason.
* **Paused under review**: donate disabled; banner shows (13.6).

**AC‑DN‑1:** Amount input validates whole dollars ≥ $5; below $5 shows inline error and disables Donate.  
**AC‑DN‑2:** Clicking Donate respects Section 14’s login/register flow and preserves amount and referral code.  
**AC‑DN‑3:** COI enforcement happens **before** redirecting to checkout.

**13.4 Gallery (images + video)**

* **Carousel** with thumbnails; supports images (jpg/png/webp) and embeds (YouTube/Vimeo).
* First item can be a **feature image**; aspect 16:9; lazy‑load offscreen items; swipe on mobile.
* **Alt text** required and read by screen readers; videos don’t autoplay; click to play.
* **Zoom** lightbox on image click; caption from alt text.

**AC‑GAL‑1:** Enforce per‑file and per‑campaign limits set in 12.C.  
**AC‑GAL‑2:** Keyboard accessible (left/right to navigate; Esc to close lightbox).

**13.5 Story, FAQ, Updates**

**Story**

* Sanitized rich text (H2–H4, lists, links, blockquote). Links open new tab with rel="nofollow noopener".
* Optional short “impact” callouts (styled blockquotes).  
  **AC‑STR‑1:** 20k soft limit/30k hard cap enforced (12.B.1).

**FAQ**

* Accordion list with expand/collapse; hyperlinks allowed; up to ~50 items.  
  **AC‑FAQ‑1:** Deep linkable to #faq and each question id.

**Updates**

* Simple feed (newest first) with timestamp and optional one image.
* **Rate limit**: 1/day (12.B.3).  
  **AC‑UPD‑1:** “View all updates” loads pagination; organizer deletions are logged (admin audit).

*(Comments are Phase‑2; not part of MVP.)*

**13.6 Global banners & page states**

**States & banners**

* **Live (KWR/AoN)** — normal state.
* **Paused: Under review** — Banner: “This campaign is temporarily unavailable while we review a report.” Donate disabled; modules visible.
* **Ended (KWR)** — Banner: “This campaign ended on {date}.” Donate disabled; totals frozen.
* **Ended — Not funded (AoN)** — Banner: “This all‑or‑nothing campaign didn’t meet its goal. All donations were automatically refunded.”
* **Suspended** — Not discoverable; direct URL shows limited view with banner; donate disabled.
* **Removed** — Return 410 with “Campaign not available” page and browse links.

**AC‑STATE‑1:** Ended KWR can still show total raised and team leaderboard (frozen).  
**AC‑STATE‑2:** Suspended state removes from discovery (16.11) and shows banner when accessed directly.

**13.7 Organizer card**

* **Avatar + badges** (verified user/org/nonprofit).
* **Organizer name** (clickable), **Member since {date}**, **City, State**, **Website** (optional).
* **CTA:** **View profile** (to public profile) and **Message** (Phase‑2; respects DM policy).
* **Disclosure** (compact): “Funds are delivered to the organizer. Rewards are provided by the organizer; not guaranteed by the platform.”

**AC‑ORG‑1:** Profile link always visible; Message visible only if their DM policy allows.

**13.8 Team leaderboard (optional module)**

* Toggle controlled in Team settings (12.J).
* Table: Rank • Member (clickable to user profile) • Amount raised • Donations • Conversion %.
* Sorting by amount desc; tie‑break by most recent donation time.
* Only **active** members shown; removed members hidden; totals include historical attributed donations.

**AC‑TEAM‑1:** Leaderboard hides if disabled; shows “Team fundraising” chip on card when enabled (16.5).  
**AC‑TEAM‑2:** Attribution logic per 12.J.3 (last touch; refunds reduce totals).

**13.9 Share module**

* Buttons: Facebook, X/Twitter, LinkedIn, **Copy link**, **QR code** (download PNG).
* Use OG tags (16.10) and referral parameters if a member link was used to arrive.
* Tooltip text: “Share to help this campaign reach more people.”

**AC‑SHR‑1:** Copy writes clean URL (keeps ref= if present); toast confirms.

**13.10 Report this campaign (donors‑only)**

**Entry**: Button near footer (and compact link under Donate widget).  
**Eligibility**: Must be a **logged‑in donor** (of any campaign, per your policy), or we can require donor of **this** campaign only.  
**(Choose)**: We’ll use your earlier policy—**donors‑only (any campaign)**.

**Modal fields**

* **Reasons** (required; multi‑select): Fraud/Misrepresentation; Prohibited content; Hate/Harassment; Privacy/Impersonation; Spam/Scam; Unsafe medical claims; Other (free text).
* **Details** (textarea)
* **Attachments** (optional): pdf/jpg/png ≤ 5MB (virus‑scanned)

**Outcome**

* Creates a **Moderation case** (20.B) with severity routing; shows thank‑you message.

**AC‑RPT‑1:** If user not eligible, clicking “Report” opens login → returns to modal.  
**AC‑RPT‑2:** Organizer is notified only when a decision is made, not on raw reports.

**13.11 Related campaigns**

* Grid of 6 items beneath main content; logic from 16.6 (category/tags/location + curated mix).  
  **AC‑REL‑1:** Exclude suspended/removed; include ended campaigns only if user toggles “Include ended” on site‑wide (16.3).

**13.12 Accessibility & performance**

* **WCAG 2.2 AA**:
  + All interactive elements keyboard navigable; visible focus; ARIA labels for icons.
  + Alt text on images; captions optional; contrast ratio ≥ 4.5:1.
* **Performance**:
  + LCP ≤ 2.5s (first meaningful image or title), lazy‑load non‑critical images, defer non‑critical JS, preconnect to CDN/payment origin.
  + Use srcset and modern formats; avoid layout shift on sticky donate.

**AC‑A11Y‑1:** Lighthouse ≥ 90 Accessibility; axe core checks pass on key flows.  
**AC‑PERF‑1:** CLS ≤ 0.1; TBT ≤ 200ms on mid‑range mobile.

**13.13 Live updates (progress)**

* When donations arrive while page is open, update **raised**, **% funded**, **donors count**, and **leaderboard** (if visible).
* Throttle to once every 5 seconds; animate count‑up; announce change to screen readers via polite live region.

**AC‑LIVE‑1:** Real‑time progress updates without page reload; no visual jitter.

**13.14 Analytics & event tracking**

Fire analytics events (names consistent with 20.T builder):

* campaign\_page\_view, donate\_cta\_click, donate\_amount\_preset\_click, donate\_other\_amount\_focus,
* share\_click (channel), copy\_link, qr\_download,
* report\_open, report\_submit,
* gallery\_next, update\_expand, faq\_expand,
* team\_leaderboard\_view, organizer\_profile\_click.

**AC‑ANL‑1:** UTM/referral codes persist into checkout; events include campaign\_id, funding\_model, viewer\_role (anon|logged\_in|affiliated).

**13.15 Error & edge states**

* **Media missing**: default placeholder image with alt text “Campaign image placeholder”.
* **Goal change upward**: show subtle badge “Goal updated on {date}” (policy allows once, upward only).
* **Deadline extension (KWR only)**: show “Deadline extended to {new date}” chip (1x allowed, 14 days max).
* **Overfunded**: progress bar capped visually at 100%; chip “100%+ funded”.
* **Blocked donation (COI)**: show affiliated block copy near donate widget.

**AC‑EDGE‑1:** All chips have tooltips linking to KB articles.

**13.16 Microcopy (ready to ship)**

* **Donate button**: “Donate”
* **Min error**: “Minimum donation is $5.”
* **Whole dollars**: “Enter a whole‑dollar amount.”
* **COI block**: “You’re part of this campaign’s team. Only the campaign owner can donate here.”
* **AoN chip**: “Charged now; automatically refunded if the goal isn’t met by {deadline}.”
* **Paused banner**: “This campaign is temporarily unavailable while we review a report.”
* **Not funded banner**: “This all‑or‑nothing campaign didn’t meet its goal. All donations were refunded.”
* **Share tooltip**: “Share to help this campaign reach more people.”

**13.17 Data model & rendering notes**

* Page fetch joins: Campaign, Organizer (User/Org), Media, RewardTier (for claim copy), TeamMember (if leaderboard enabled), Progress snapshot, Badges.
* Respect privacy for donors in “Recent donors” (if added later): anonymous donors show “Anonymous” only.
* Expose funding\_model\_snapshot in client to render AoN copy confidently.

**13.18 Acceptance Criteria (summary)**

* **Layout** responsive with sticky donate and bottom mobile bar; keyboard order correct.
* **Header** shows correct badges, organizer link, progress, AoN tooltip.
* **Donate widget** enforces min $5, whole dollars, COI rules, and routes into Section 14 flow with preserved amount/referral.
* **Gallery/Story/FAQ/Updates** match rules in Section 12; accessible; sanitized.
* **Banners & states** render correctly for Paused, Ended (KWR), Not funded (AoN), Suspended.
* **Organizer card** links to public profile; DM CTA respects policy.
* **Team leaderboard** renders if enabled; hidden if off; totals reflect refunds.
* **Share** controls copy correct link (with ref=); QR download works.
* **Report** is donors‑only; creates moderation case; attachments scanned.
* **Related** list computed and excludes suspended/removed.
* **Accessibility/Performance** budgets met; live updates smooth.
* **Analytics** fire with correct metadata; UTMs/refs preserved.

**13.19 Roadmap hooks (Phase‑2)**

* Donor‑only **comments** under Updates with moderation tools.
* Public **“Follow” organizer/campaign** → Notifications (Section 18).
* **Matching gifts** badge/callout.
* **Multi‑currency display** (while charging USD).
* **Localization** and RTL layouts.
* **Map** module if location is specific (e.g., disaster relief area).

# Section 13B — Public Campaign Page

**Scope:** Desktop/mobile layouts and modules, sticky donate UX, progress math, gallery, story/FAQ/updates, rewards display, team leaderboard, recent donors & donor messages, share/report, states (live/ended/suspended/AoN not funded), SEO/OG/structured data, performance & a11y standards, analytics events, data bindings, acceptance criteria, and QA.

**Depends on:** §0 policies; §4 (UX/A11y/Perf); §5 (Risk/Moderation); §6 (Privacy/Legal); §7 (APIs/Webhooks); §8 (DB); §10 (Portal); §11 (KYC/KYB); §12 (Campaign creation, media, rewards, team); §14 (Checkout); §16 (Discovery); §18 (Notifications); §20 (Admin); §21–22 (Ops/QA).

## 13.0 Goals & principles

* **Clarity first:** What is this about, who runs it, how much is needed, how to help.
* **Trust by design:** Visible verification badges; transparent AoN/KWR labels; donors‑only reporting.
* **Conversion on mobile:** Sticky donate CTA; fast LCP; simple modals/drawers.
* **A11y:** WCAG 2.2 AA; full keyboard & SR support.
* **Performance:** Meet §4.6 budgets (LCP ≤ 2.5s P75; TBT ≤ 200ms; CLS ≤ 0.1).

## 13.1 Routing, URL & SSR/CSR strategy

* **Route:** /c/{slug}-{shortId} (e.g., /c/help-jamie-abc123)
  + {slug} mutable; {shortId} immutable to avoid broken links when title changes.
* **Canonical:** Points to latest slug for the same {shortId}.
* **SSR:** Server‑render **above‑the‑fold** (hero, title, organizer, progress, primary CTA) for LCP & SEO.  
  Hydrate **Donate widget** and **Gallery** progressively.
* **Personalization zones (CSR only):** “Donate” widget state, recent donors/messages, DM button visibility, report modal gating, team leaderboard share links.
* **Caching:**
  + **Static shell** (SSR) cache 60s;
  + **Dynamic progress counters** via SSE or polling every 10–15s (backoff on idle/tab hidden).
  + ETags for story and media; conditional requests.

## 13.2 Page layout (desktop & mobile)

### Desktop (≥1024px)

* **Left (66%)**: Cover/gallery → Title & badges → Organizer strip → Progress module → Donate widget (inline) → Team leaderboard (optional) → Story → FAQ → Updates → Recent donors & messages → Share.
* **Right (34%) sticky column**: Donate widget (sticks after 600px scroll) with progress mini‑bar + Report this campaign (donors‑only) link.

### Mobile (<1024px)

* **Top:** Hero cover with Donate floating CTA (bottom sticky bar).
* **Body order:** Title & badges → Organizer strip → Progress → Donate sheet trigger → Team leaderboard (optional) → Gallery → Story → FAQ → Updates → Recent donors & messages → Share → Report (donors‑only).
* **Donate:** opens a **bottom sheet** (Section 14) with amount chips + custom amount, tip, cover fees, terms, Continue.

**A11y:** Skip link “Skip to campaign details” before hero; focus moves to <h1> on route change.

## 13.3 Hero & header strip

**13.3.1 Cover**

* Aspect 16:9; responsive srcset (mobile ≤ 500KB).
* If video at first position, show **poster image**; click to play (no autoplay).
* Alt text from §12.C.1; required.

**13.3.2 Title & badges**

* <h1>{campaign\_title}</h1>.
* Badges (chips):
  + **Verified** (tooltip: “Verified: email, phone, ID”)
  + **Verified Nonprofit** (if EIN matched; tooltip: “Verified nonprofit via IRS”)
  + **KWR** or **AoN**
  + Category chip; location (City, ST)
* **A11y:** badges have aria-label with explanations.

**13.3.3 Organizer strip**

* Avatar + display name (link to **entity profile**, §10.T) + “Contact organizer” DM button.
* Tooltip or inline text for team: “Organized by {Name} with {N} teammates” (if team enabled).

**13.3.4 Quick meta**

* Start date, End date (localized), Time left (days/hours), Updated {relative time} if recent.

## 13.4 Progress module

* **Elements:** Raised "$X of $Goal" + **percent** + **progress bar** (text alternative announces exact values) + **Supporters count** (unique donors) + **Days left**.
* **AoN banner:** Chip with tooltip “All‑or‑Nothing: charged now; refunded automatically if goal isn’t met by {deadline}.”
* **KWR banner:** Chip “Keep‑What‑Raised”.
* **Live updates:** via SSE/polling; smooth animation ≤ 150ms (respect reduced motion).
* **Edge copy:** If goal updated (KWR), show footnote: “Goal updated on {date}.”

**AC‑PROG‑1:** Numbers match ledger in real‑time within 60s (webhook SLA §7).  
**AC‑PROG‑2:** Screen reader announces percent & amounts; bar has aria-valuenow.

## 13.5 Donate widget (on‑page)

* **Amount:** Quick chips ($25/$50/$100/$250) + **custom** (whole dollars; min $5).
* **Tip & Cover fees:** per §14.B/C config; tooltips with sample math.
* **Privacy:** toggles: **Hide my name publicly** (default ON per §14.E.23), **Donate anonymously** (explainer that rewards & messaging will be unavailable if anonymous).
* **Terms/Policies:** required checkbox (links to ToS/Privacy/Community Guidelines).
* **CTA:** “Donate” → triggers §14 checkout.
* **COI guard:** If viewer is **Team Member/Co‑Lead/Support** of this campaign, **disable CTA** with copy: “You’re part of this campaign’s team. Only the campaign owner can donate here.”
* **State when disabled:**
  + Suspended: “Temporarily unavailable while under review.”
  + Ended (KWR): “Campaign ended.”
  + AoN not funded after deadline: “Not funded — donations refunded.”

**Mobile:** bottom sticky **Donate** bar shows total chip (amount if selected) + tap to open donate sheet.

**AC‑DW‑1:** Whole dollar & min guardrails; terms must be checked; COI block enforced.  
**AC‑DW‑2:** AoN disclosure visible before confirm.

## 13.6 Gallery (images & video)

* **Carousel** (keyboard & swipe): arrows, bullets, thumbnails optional.
* **Images**: zoomable lightbox; alt text; ESC closes; no background scroll.
* **Video embeds**: YouTube/Vimeo oEmbed; click‑to‑play; captions encouraged; no autoplay.
* **Error fallback:** “This video is unavailable.”
* **Counts:** Up to 15 images, 5 videos (from §12.C).
* **Perf:** Lazy load beyond first 1–2 items.

**AC‑GAL‑1:** Fully keyboard accessible; focus trap in lightbox; close returns focus to invoker.

## 13.7 Story, FAQ & Updates

**Story (RTE subset)**

* Sanitize links (https, rel="nofollow noopener").
* Collapsed after 600–800px on mobile with “Read more”.
* TOC anchors for long stories (optional).
* PHI/PII caution copy (subtle) per §6.8 (no medical records).

**FAQ**

* Accordion; reorder preserved; deep links supported (#faq-q{n}).

**Updates**

* Chronological (newest first); **max 1/day** (from §12.B.3).
* Each: timestamp, text, optional image; deletions logged (not shown publicly).

**AC‑CONTENT‑1:** No scripts/iframes except vetted video; links strip tracking params.  
**AC‑CONTENT‑2:** “Read more” toggles are keyboardable and SR‑announced.

## 13.8 Rewards module (if organizer added tiers)

* **Card list** of tiers (1–6):
  + **Amount** (ascending), **Title**, **Short description**, **Delivery type (Physical/Digital)**, **Est. delivery** (Month/Year), **US‑only** badge if shipping region restricted, **Quantity left** (if capped).
* **Sold out** tiers disabled with “Sold out” label.
* **AoN note:** “Rewards fulfilled only if funding goal is met.”
* **Info lines:** “Physical rewards require your name & address after donation.”
* **Action:** Selecting a tier **sets donation amount** and scrolls user to Donate widget (or opens sheet on mobile).
* **Options (e.g., Size)** are **not** selected here (set during **Reward claim** after donation).

**AC‑RWD‑1:** Tiers respect ascending rule; sold‑out tiers disabled; setting a tier amount updates donate amount.

## 13.9 Team leaderboard (optional, per §12.J)

* Toggle controlled by organizer (on/off).
* **Display:** top 5 members by amount raised (attribution), with “See all” → modal or dedicated page.
* **Each entry:** name/avatar, total raised, **Share** button (copies their personal ref link).
* **Donate via member** (optional): deep‑link ?ref=memberCode applied to Donate widget.

**AC‑TEAM‑1:** Removing a member keeps their historical totals; “invalid link” shown for old ref codes.

## 13.10 Recent donors & messages

* **Purpose:** Social proof while honoring privacy.
* **Items shown:** 10 most recent donations (rolling), **name display rules**:
  + **Anonymous donor** → show “Anonymous”.
  + **Hide name publicly** → show first initial + last initial (e.g., “J. S.”).
  + Otherwise → full display name.
* **Message (optional)**: If donor left a message (≤280 chars), show below name.
* **Amounts:** **Not shown publicly in MVP** (privacy‑friendly).
* **Timestamps:** relative (“2h ago”).
* **CTA:** “Send a message” (DM) for donors (visible when logged‑in donor viewing their own donation via portal link).
* **Load more:** fetch next 10.

**AC‑DONORS‑1:** Obey privacy flags (anonymous vs hide name).  
**AC‑DONORS‑2:** Messages filtered for profanity/links per §14.E.21.

## 13.11 Share & report

**Share module**

* Buttons: **Copy link**, Facebook, X/Twitter, LinkedIn; show **share as me** variant when arriving from team page (includes ref code).
* On copy: short confirmation toast.

**Report this campaign (donors‑only)**

* Button opens modal **only if viewer is a donor (any campaign)**.
* **Reasons (select)**: Suspected fraud / Prohibited content (adult/weapons/raffle) / Hate or harassment / Privacy risk (PII/PHI) / Misleading or duplicate / IP infringement / Other.
* **Details**: free text; optional screenshot/URL; must include at least 20 chars.
* **Result:** creates **Moderation case** (§20.B), donations paused only if staff suspends.

**AC‑REPORT‑1:** Non‑donors see tooltip “Only donors can report campaigns.”  
**AC‑REPORT‑2:** Reports rate‑limited (3/day).

## 13.12 States & banners

| **State** | **Visual treatment** | **Donate widget** |
| --- | --- | --- |
| **Live** | Normal | Enabled |
| **Paused (Under Review)** | Yellow banner “Temporarily unavailable while we review a report.” | Disabled |
| **Ended — KWR** | Gray banner “Campaign ended {date}.” | Disabled |
| **AoN — Not Funded** | Red banner “Not funded — donations refunded.” | Disabled |
| **AoN — Funded** | Green banner “Goal met on {date}!” | Enabled until end date reached, then Ended |
| **Goal updated** (KWR) | Sub note in progress | — |
| **Suspended** (T&S) | Red banner “This campaign has been suspended for policy reasons.” | Disabled |
| **Unpublished** | 404 for public; preview link for owner shows purple “Preview” banner | Disabled |

**AC‑STATE‑1:** State logic consistent with §12.H & §20.B actions.

## 13.13 SEO, social & structured data

**Head tags**

* <title>{campaign\_title} — {city, ST} | {brand}</title>
* <meta name="description" content="{short\_desc (≤160 chars)}">
* Canonical to latest slug; og:\* and twitter:\* tags:
  + og:title, og:description, og:image (cover), og:url, og:type=website
  + twitter:card=summary\_large\_image
* **Noindex** for Suspended and Unpublished; **410** for deleted campaigns.

**Structured data (JSON‑LD)**

* WebPage + BreadcrumbList
* CreativeWork for the campaign with name, description, startDate, endDate, location, creator (Person/Organization), isAccessibleForFree: true
* Optional DonateAction with target URL and recipient (Person/Organization).

**Sitemaps**

* Campaigns included when **Live**; removed or marked **lastmod** on Ended.

**AC‑SEO‑1:** LCP element is cover image (optimized).  
**AC‑SEO‑2:** OG image uses proper aspect (1.91:1 or 1200×630); fallback if none.

## 13.14 Accessibility & performance

* **Keyboard:** All interactive elements reachable; focus visible; close modals with ESC; sticky donate accessible (no focus trap).
* **SR:** Progress bar announces values; gallery images have alt text; update timestamps read correctly; badges read with explanations.
* **Perf:**
  + Code‑split gallery & updates; lazy load images; avoid layout shifts; preconnect to Stripe only on Donate open.
  + Resource hints: preload cover image, dns-prefetch to CDN; defer all third‑party scripts.

**AC‑A11Y‑PERF‑1:** Page meets §4.6 budgets; Lighthouse ≥ 90 (Performance & A11y) on campaign route.

## 13.15 Analytics & events (to §20.T)

* campaign\_page\_view{campaign\_id, category, state, is\_aon, loc\_state}
* donate\_cta\_click{position: hero|sticky|rewards, amount\_preset?, ref\_code?}
* share\_click{channel} / copy\_link
* gallery\_nav{index, type:image|video}
* faq\_toggle{q\_id}
* update\_expand{id}
* reward\_card\_click{tier\_id, amount}
* team\_leaderboard\_view|see\_all|share\_ref{member\_id}
* report\_open|submit{reason}
* dm\_open\_from\_campaign

**Dashboards:** Conversion funnel (view → donate start), share CTRs, reward click → donate conversion, report rates, AoN vs KWR performance, team attribution.

## 13.16 Data model & bindings (to §8)

* **Reads from:**  
  campaign, campaign\_media, campaign\_update, reward\_tier, team\_member, donation (public projection), user\_profile (public projection), faq.
* **Derived projections:**
  + campaign\_public view includes: organizer display name, verification flags, totals, supporters\_count, progress %, days left, team\_enabled.
  + donation\_public view enforces privacy flags for donors/messages.
* **Live updates:**
  + Webhook events (payment\_intent.succeeded|refund|dispute) update counters; push via SSE.
  + Reward tier “Sold out” flips on donation counts hitting limit.

**Indexes:**

* campaign (status, end\_date DESC), donation (campaign\_id, created\_at DESC), team\_member (campaign\_id, amount\_raised).

## 13.17 Acceptance Criteria (summary)

1. **Layout & modules** render as specified on desktop & mobile; donate sticky/CTA behaves per scroll rules.
2. **Progress**, **supporters**, and **days left** are accurate within 60s of new events.
3. **Donate widget** enforces min/whole‑dollar, terms, COI block; AoN disclosure shown.
4. **Gallery** is accessible and performant; no autoplay; error fallback for removed videos.
5. **Story/FAQ/Updates** render sanitized content; long content collapses correctly.
6. **Rewards** show tier cards with sold‑out and US‑only notices; selecting a tier sets amount.
7. **Team leaderboard** appears only when enabled; ref links work; historical attribution retained.
8. **Recent donors/messages** respect privacy flags; profanity filtered.
9. **Share** works; ref codes propagate; **Report** is donors‑only and creates moderation cases.
10. **States** (live/paused/ended/aon not funded/suspended) show correct banners and enable/disable donate correctly.
11. **SEO/OG/Structured data** emit correct tags; canonical & sitemaps correct; suspended/unpublished noindexed.
12. **A11y & Perf** meet Section 4 budgets; keyboard and SR checks pass.
13. **Analytics** fire for key interactions; dashboards can be built with data.

## 13.18 QA checklist (tie to §22)

* Mobile & desktop hero LCP times; sticky donate behavior; reduced motion respected.
* Donate min $5 and whole dollars enforced; terms required; COI block for team members.
* AoN banner present at header & donate; AoN failure flips to “Not funded” with auto‑refund banner.
* Progress updates live when a test donation/refund/dispute occurs; SSE/poll works.
* Gallery keyboard navigation; lightbox focus trap; video fallback shows when removed.
* Story links https, rel attributes set; “Read more” a11y works.
* Rewards: sold‑out flips when quantity hit; tier click sets amount; messages reflect shipping note.
* Team: leaderboard toggled off/on; referral link adds ?ref= and attribution flows to checkout.
* Donors/messages: anonymity & hide‑name rules; profanity filter; load‑more works.
* Share buttons: correct URLs & OG; copy toast; ref codes preserved.
* Report modal: donors‑only gating; reason required; creates moderation case.
* State banners: Paused, Ended, Suspended; Donate disabled with correct copy.
* SEO: canonical, OG image, JSON‑LD valid; Suspended noindex.
* Analytics events logged with correct payloads.

## 13.19 Microcopy kit (ready to ship)

* **AoN chip tooltip:** “All‑or‑Nothing: charged now; refunded automatically if the goal isn’t met by {date}.”
* **COI block (donate):** “You’re part of this campaign’s team. Only the campaign owner can donate here.”
* **Donate privacy toggles:**
  + “Hide my name publicly (organizer can still contact me for rewards)”
  + “Donate anonymously (rewards and messaging unavailable)”
* **Rewards note:** “Physical rewards require your name and a US shipping address after donation.”
* **Paused banner:** “Temporarily unavailable while we review a report.”
* **Not funded banner:** “Not funded — all donations have been refunded.”
* **Sold out (tier):** “This reward tier is fully claimed.”
* **Share toast:** “Link copied.”
* **Report modal subtitle:** “Only donors can file reports. Tell us what’s wrong and include details.”

## 13.20 Roadmap (Phase‑2)

* Public **donation amount opt‑in** (“Show amount publicly”) at checkout.
* **Follower** feature (donors subscribe to updates without donating again).
* **Comments** (moderated, donors‑only) with anti‑abuse controls.
* **Multi‑image lightbox annotations** and **video transcripts** (a11y).
* **Map module** for campaigns with a specific location (optional).

**Section 14 — Donation & Checkout Flow**

**14.0 Scope & dependencies**

* Covers: entry points, session gating, amount presets, fee/tip UX, payment rails, identity/privacy inputs, reward-claim handoff, confirmations, retries, fraud controls, analytics, receipts/tax, refund requests, admin views, accessibility, copy, formulas.
* Depends on: Section 12 (rewards, AoN/KWR labels, team referral), Section 0 (policies, tips, cover-fees), Section 11 (KYC), Section 18 (notifications).

**14.1 Flow architecture**

**Default path (no guest checkout):**

1. **Campaign page** → Donate CTA
2. **Auth gate** (Login / Register)
3. **Checkout** (Amount & options → Payment → Confirm)
4. **Post‑payment** → (a) **Reward Claim** if tier‑eligible, or (b) **Thank‑you**
5. **Receipts & notifications** → donor, organizer

**Progress bar:** **Amount → Details → Pay → Done** (fixed across desktop/mobile).

**14.2 Entry points & session gating**

**Entry points (enabled):**

* Donate button on **campaign page** (primary).
* Donate CTA on **campaign cards** in listings (pre‑fills amount if chip clicked).
* **Sticky header** Donate on public campaign page while scrolling.
* Donate CTA on **team‑member pages** (pre‑attributes to the member).
* Donate CTA in **campaign updates** posts.

**Deep‑linking:** /donate/:campaignId?amount=XX&member=YY&utm=... pre‑fills amount and attributes to team member if present.

**Single active session (per user × campaign):**

* Opening a second checkout tab for the **same campaign** shows **“Another checkout is in progress”** with options:
  + **Take over** (closes prior session, issues a new idempotency key).
  + **Go back to campaign**.
* **Timeout:** checkout session expires after **15 minutes** of inactivity.

**AC**

* AC‑ENTRY‑1: All entry points respect auth gate; deep‑link preserves prefilled amount and referral.
* AC‑SESSION‑1: Only one active checkout session per user × campaign; takeover flows work on desktop/mobile.

**14.3 Amount, presets & guardrails**

* **Amount field:** whole dollars only; numeric keypad on mobile.
* **Presets:** **$25 / $50 / $100 / $250** chips + **Other** (focuses amount field).
* **Express chips with reward labels:** When a tier is exactly matched, chip shows **“$50 — Signed Book”**.
* **Soft confirmation:** If amount ≥ **$10,000**, show “Please confirm your $X donation” modal.
* **Velocity limits (anti‑fraud):**
  + **Max per transaction:** **$20,000**
  + **Max per user/day (rolling 24h):** **$20,000**
  + **Max per user/30 days:** **$100,000**  
    (Admin‑configurable; errors show friendly copy.)

**AC**

* AC‑AMT‑1: Reject amounts < **$5** with clear inline error.
* AC‑AMT‑2: Whole dollars enforced; chips update amount field.

**14.4 Tip & “cover fees” UX**

* **Tip selector:** buttons **10% / 15% / 20% / Custom / No tip**; **15% preselected**; remember last choice per user.
* **Placement:** below amount, above payment methods.
* **Cover fees toggle:** **Default ON**; one‑line fee math summary with **hover tooltip** (“Estimated processing fees; you can change this anytime.”).
* **Fee formula:** admin‑configurable (e.g., 2.9% + $0.30); see **Math Appendix**.

**AC**

* AC‑TIP‑1: Selecting **Custom** opens a field; validates ≥ $0.
* AC‑FEES‑1: Toggle ON/OFF updates “Net to campaign” preview immediately.

**14.5 Payment methods (Stripe)**

* **Cards:** Visa, MasterCard, AmEx, Discover.
* **Wallets:** **Apple Pay** and **Google Pay** (device‑gated).
* **Stripe Link:** enabled; “Save with Link” opt‑in during pay.
* **Save card** checkbox (for future use): available, **unchecked by default**.
* **3DS**: step‑up only when Stripe requires / high risk.
* **Non‑US cards:** **Allowed**; USD‑only; apply extra risk scoring.

**Not in MVP:** ACH/Bank pay (Phase‑2).

**AC**

* AC‑PAY‑1: Apple/Google Pay shown only when supported.
* AC‑PAY‑2: 3DS modal resumes checkout correctly on success/abandon.

**14.6 Identity, privacy & donor inputs**

* **Hide my name publicly** (organizer still gets contact; **rewards allowed**).
* **Donate anonymously** (no contact shared; **rewards unavailable**).
* **Donor message** (≤ **280 chars**; profanity/URL filter).
* **Dedication**: “In honor of / In memory of” (optional text field).
* **Subscribe to organizer updates**: **Default ON**; can be changed later.
* **Consent:** required checkbox referencing **ToS, Privacy, Community Guidelines**.

**AC**

* AC‑ID‑1: Choosing “Donate anonymously” auto‑disables Reward Claim path and shows an explanation tooltip.

**14.7 Payment step & review**

* **Order summary panel** updates in real time: Donation, Tip, **Estimated fees (if covering)**, **Total charge**, **Net to campaign**.
* **AoN banner (when applicable):** “You will be charged now. If the goal isn’t met by **{deadline}**, you’ll be **automatically refunded**.”

**AC**

* AC‑REV‑1: Cannot proceed without consent checkbox.
* AC‑REV‑2: For AoN, banner also appears on email receipt.

**14.8 Reward claim handoff (if tier‑eligible)**

* **Immediate redirect** to **Reward Claim** page after payment; **“Finish later”** link goes to Thank‑you page and adds a portal banner reminder.
* **Address validation:** USPS/Smarty inline; **PO Boxes allowed**.
* **Digital rewards:** may specify **gift recipient email** (optional).
* **Edit cutoff:** shipping info **locks** when organizer moves status to **Pending** (Section 12).

**AC**

* AC‑RC‑1: If donor abandons claim, a **persistent portal banner** appears until claimed or opted‑out.
* AC‑RC‑2: Anonymous donors bypass claim page and see a note explaining why.

**14.9 Confirmation & notifications**

**Thank‑you page modules (always):**

* Success message + **receipt summary**
* **Share** buttons (Facebook, X/Twitter, LinkedIn) + **Copy link**
* “Follow campaign updates” toggle (reflects subscription state)
* If tier‑eligible: **“Finish Reward Claim”** prompt
* “View **Donation History**” link

**Receipts & confirmations:**

* **Email** receipt immediately; includes AoN rule if applicable.
* **SMS** confirmation (short), linking to the receipt page.

**AC**

* AC‑CONF‑1: Team referral attribution included in receipt if present.

**14.10 Error handling & retries**

* **Network/timeouts:** auto‑retry once; then show “We couldn’t process that—please try again or use a different method.”
* **Idempotency:** multiple rapid clicks/tabs deduped by key; only one charge created.
* **3DS abandoned:** portal shows “Continue your payment” link for **24 hours**.

**AC**

* AC‑ERR‑1: Duplicate prevention verified (one charge, one receipt).
* AC‑ERR‑2: Abandoned 3DS visible in **Donation History** as “Action required.”

**14.11 Fraud & abuse controls**

* **Velocity checks:** **3 donations/min**, **10/hour** per user/device/IP (configurable).
* **Same‑card, multiple accounts**: soft‑block + review flag.
* **Disposable emails:** warn & allow; higher risk score.
* **Message/dedication filters:** profanity list + URL strip/mask.
* **Organizer donating to own campaign:** allowed, flagged for review (anti‑wash).

**AC**

* AC‑FRD‑1: Review flags create a case for Moderation/Finance Ops with the donation attached.

**14.12 Data & analytics**

* **Capture UTM** params + **team referral** on the Donation record.
* **Events tracked:** open donate, preset click, amount change, tip change, cover-fees toggle, payment method opened, 3DS shown, payment success/fail, reward claim start/submit, share click.
* **Organizer analytics** receive aggregates (as per Section 12).

**AC**

* AC‑DATA‑1: Events include campaign\_id, user\_id, session\_id, referral\_member\_id (if any).

**14.13 Receipts & tax**

* **Breakdown:** donation, tip, fees (if covered), total charged, net to campaign, funding model (KWR/AoN), reward tier (if any).
* **Tax:** personal campaigns not tax‑deductible; charities **may** be—add advisory that **rewards/benefits can reduce deductibility**.
* **Downloadable PDF** in portal.

**AC**

* AC‑RCT‑1: PDF mirrors receipt page; includes unique receipt ID.

**14.14 Refund requests & windows**

* **Donor UI:** “Request a refund” on the donation detail page → creates a ticket visible to Organizer & Admin.
* **Organizer self‑serve**: within **24 hours** and **≤ $1,000**, organizer can refund without Finance Ops; beyond that requires Finance Ops approval.
* **Partial refunds:** supported; donor receives updated receipt.

**AC**

* AC‑RFND‑1: AoN **Not Funded** → system auto‑refunds all donations; donors notified.

**14.15 Admin & support views**

* **Donation detail:** risk score, card BIN info, 3DS outcome, gateway logs, UTM, team attribution, AoN/KWR snapshot, attempts/retries.
* **Bulk AoN refund management:** monitor and re‑issue failed refunds.
* **Support agent view:** quick links to donor, campaign, and dispute creation.

**14.16 Accessibility & performance**

* **WCAG 2.2 AA** patterns: labels, descriptions, ARIA roles for toggles/chips, focus management on errors, keyboard operability for amount and chips.
* **Performance targets:**
  + Donate click → payment elements render < **1.5 s** on 4G.
  + Autocomplete & validation < **150 ms** for perceived instant feedback.

**14.17 Microcopy & disclosures (ready for UI)**

* **Cover fees tooltip:** “Helps the campaign receive your full intended amount.”
* **Tip explainer:** “Optional tip supports platform operations.”
* **Hide name:** “Your name will be hidden publicly; the organizer can still contact you for rewards.”
* **Anonymous:** “Organizer will not receive your contact details. Rewards are unavailable for anonymous donations.”
* **AoN banner:** “Charged now; automatically refunded if the goal isn’t met by {deadline}.”
* **High‑amount confirm:** “Please confirm this **${amount}** donation.”
* **Consent checkbox:** “I agree to the Terms, Privacy Policy, and Community Guidelines.”

**14.18 Math appendix (cover fees & totals)**

Let:

* **D** = donation amount (whole dollars)
* **T** = tip amount (could be percent‑based; round to nearest **$0.01**)
* **p** = processor percentage fee (e.g., **0.029**)
* **f** = fixed fee (e.g., **$0.30**)
* **C** = donor covers fees **ON** (true/false)

**If C = OFF**

* **Total charge** = **D + T**
* **Processor fees** charged on total = **p·(D+T) + f**
* **Net to campaign** ≈ **D − [p·(D+T) + f]** (platform absorbs the difference policy‑wise as configured)

**If C = ON (gross‑up to target D net to campaign)**  
We gross‑up the charge so that **campaign nets D** after fees on the *entire* charge.

1. We target a donor charge **X** such that **X − (p·X + f) − T = D**
2. Solve for **X**:
   * **X(1 − p) − f − T = D**
   * **X = (D + f + T) / (1 − p)**
3. **Total charge** = **X** (rounded to **$0.01**)
4. **Cover‑fees line item** shown to donor = **X − (D + T)** (labeled “Estimated fees”)
5. **Net to campaign** = **D** (± a penny due to rounding)

**Admin switch (optional)**: If you prefer to cover fees on **donation only** (not tip), replace **T** with **0** in the numerator (we’ll keep both modes in config; default is **cover fees on donation only**).  
**UI copy** reflects whichever mode you select.

**Examples (donation only mode, 2.9% + $0.30):**

* D = $100, T = $15 → X = (100 + 0.30) / (1 − 0.029) + 15 = $118.78 (donor charge)
* Cover‑fees line ≈ $3.78; Net to campaign ≈ $100.00

**14.19 Acceptance criteria summary (engine‑ready)**

* **Auth gate:** no guest checkout; deep‑links preserved.
* **Session control:** one active checkout per user×campaign; takeover flow.
* **Amounts:** whole dollars; presets; min $5; soft confirm ≥ $10k; per‑txn cap $20k; daily cap $20k; 30‑day cap $100k.
* **Tips/fees:** 10/15/20/Custom/No tip, 15% default; cover fees default ON; fee math hover; instant net preview.
* **Payments:** Cards + Apple/Google Pay + Stripe Link; save card unchecked; 3DS step‑up; non‑US cards allowed.
* **Privacy:** hide name vs anonymous with tooltips and reward logic.
* **Consent:** required checkbox (ToS/Privacy/Guidelines).
* **AoN clarity:** banner at checkout + in receipt.
* **Reward handoff:** immediate with “Finish later”; USPS/Smarty validation; gift recipient for digital; lock after Pending.
* **Confirmations:** thank‑you page with share; email + SMS receipts.
* **Errors:** one retry on timeout; idempotency; 24‑hour “continue payment” for 3DS.
* **Fraud:** velocity limits; same‑card multi‑account soft‑block; disposable email warning; message filters; self‑donation flagged.
* **Analytics:** events + UTM + referral captured; organizer dashboards receive aggregates.
* **Receipts & tax:** full breakdown; PDF; advisory on deductibility & rewards.
* **Refunds:** donor request workflow; organizer 24h ≤ $1,000 autopermission; partial refunds; AoN auto‑refunds.
* **Admin:** rich donation detail; bulk AoN management; support tooling.
* **Accessibility & performance:** WCAG 2.2 AA; <1.5s payment element render target.

# 

# Section 15 — Payouts & Cash Out

**15.0 Scope & dependencies**

* **Scope:** How funds become available, payout eligibility, holds/reserves, payout destinations, request vs automatic payout, statuses, failures/retries, statements, tax center, notifications, admin/ops, data model, and microcopy.
* **Depends on:**
  + **Section 0:** US‑only; payout at campaign end; hold 3–5 business days; min payout $50; max $50k per payout/$100k per day; organizer must be 18+; DL/ID before launch; SSN last‑4 before payout; EIN for orgs; refunds & disputes policy.
  + **Section 12:** one **campaign‑level payout recipient** (organizer for personal; organization for charity/company); team fundraising does **not** split payouts.
  + **Section 14:** receipts/fees math; anonymous donations; refunds.

**15.1 Payout model (high level)**

* **Per‑campaign balance:** Each campaign accumulates **Eligible Balance** (donations captured) minus refunds/chargebacks/adjustments.
* **Payout timing:** **At campaign end** (KWR & AoN that successfully fund), after a **3–5 business day hold** (“cooling‑off window”).
* **Payout trigger:** **Automatic payout** after the hold window **if all eligibility checks pass**; organizers **can also click “Request Payout”** once eligibility is green—this schedules the next available payout run.
* **Payout frequency:** One payout per campaign end (you can end early; doing so starts the hold window).
* **No guest payouts:** Only to verified recipients (see eligibility).

**15.2 Eligibility & checks**

**Eligibility prerequisites (must be green):**

1. **Identity:** Email & phone verified; **DL/State ID** verified.
2. **Tax:** **SSN last‑4** verified (individual) or **EIN** (organizations); Tax profile completed (see 15.8).
3. **Payout destination:** **Verified** US bank account on file.
4. **Minimum payout:** **$50** net available.
5. **Compliance & risk:** No active **Compliance Hold** (e.g., suspicious activity, unresolved reports).
6. **Campaign status:** Ended and **Eligible** (AoN funded or KWR regardless of goal).

**UI behavior**

* If any item is missing → **Cash Out** disabled with a contextual checklist and “Fix” buttons.
* Changing **bank account** or **legal name** triggers a **24‑hour security cooldown** before payout can be requested.

**Acceptance criteria (AC)**

* **AC‑ELIG‑1:** Cash Out button is enabled only when all checks are green.

**AC‑ELIG‑2:** Bank changes enforce a 24‑hour cooldown with banner + timestamp.  
  
**Eligibility prerequisites (must be green):**

1. **Identity**
   * **Email & Phone:** verified at registration (already required).
   * **Government ID:** **DL/State ID** verified **before campaign launch** (as set in Section 0/11).
2. **Tax profile**
   * **Individuals:** **SSN last‑4** verified **before payout**.
   * **Organizations/Charities:** **EIN** + business profile/authorized rep attestation.
3. **Payout destination (via Stripe)**
   * **US bank account on file**, verified through **Stripe Connect** onboarding (Express‑style).
   * Organizer manages bank details in a secure, Stripe‑hosted flow.
   * Changing bank requires **SMS OTP** + confirmation email; **24‑hour security cooldown** before payout can be requested.
4. **Minimum available balance**
   * **$50** net available (after holds/reserves).
5. **Compliance & risk (chosen for you)**
   * **No active Compliance Hold** on the **user** or **campaign**.
   * Blocking triggers (any one will block payout until reviewed):
     + Campaign flagged with **“Fraud/Misrepresentation”** or **“Prohibited content”** by **≥2** unique donors **or** by automated signals (high risk score).
     + KYC discrepancy (e.g., name mismatch on bank vs ID).
     + Open law‑enforcement or court request (rare).
   * **Non‑blocking** triggers (payout proceeds but case is created): low‑severity content reports, first‑time identity re‑checks that pass, single donor disputes under threshold.
6. **Campaign status (chosen for you)**
   * **Ended & Eligible.**
     + **KWR:** campaign ended (or manually ended early) **and** cooling‑off hold complete.
     + **AoN:** campaign ended with **Goal Met**; if **Not Funded**, donations auto‑refunded and **no payout** is created.
   * Campaign must **not** be **Suspended** or **Removed**.

**Organizer‑facing microcopy (new):**

* **Compliance Hold:** “Your payout is paused while our team reviews a potential issue. We’ll email you as soon as it’s resolved.”
* **Status not eligible:** “Payouts are available after your campaign ends and a short review period.”

**AC updates**

* **AC‑ELIG‑3:** Payout button is disabled if **Compliance Hold** is true or **Status** ≠ Ended & Eligible; checklist shows the precise blocker.
* **AC‑ELIG‑4:** When a Compliance Hold is cleared, organizer is auto‑notified and **Cash Out** re‑enabled.

## Stripe Connect implementation note (non‑technical)

* We’ll use **Stripe Connect (Express)** for organizer onboarding and bank linking. This keeps sensitive data off our servers, simplifies **1099‑K** delivery (when applicable), and gives us reliable payout statuses/events for our ledger.
* Our portal surfaces **status** and **call‑to‑action** banners; clicking “Change destination” opens the Stripe‑hosted UI.
* Name mismatches and verification failures raise **Compliance Hold** automatically in our system.

**15.3 Holds & reserves**

* **Cooling‑off window (campaign end):** **3–5 business days** (we’ll display an exact ETA based on cutoffs & holidays).
* **Operational reserve (risk control):** **0% for MVP** (simple); Admin can place **case‑by‑case reserves** (e.g., 10% for 30 days) via Compliance if needed.
* **Disputes/chargebacks post‑payout:** If a chargeback arrives after payout, the campaign wallet can become **negative**; see 15.9.

**AC**

* **AC‑HOLD‑1:** Statement shows “Hold until {date}” and a countdown.
* **AC‑HOLD‑2:** If Admin adds a reserve, organizer sees the % and release date.

**15.4 Payout destination & security**

* **Destination types:** **US bank account** (routing + account) or bank via a secure link flow.
* **Multiple banks:** Allow **one active** payout destination; organizer may replace it (old one is archived).
* **2‑step security:** Changing destination prompts **OTP** to phone and a confirmation email.
* **Name match:** If bank account holder name materially differs from organizer name or org legal name, show “Needs review” and place a **Compliance Hold**.

**AC**

* **AC‑DEST‑1:** Replace bank flow requires OTP; success banner + audit log.
* **AC‑DEST‑2:** Name mismatch flags Compliance and blocks payout until resolved.

**15.5 Cash Out flow (organizer)**

**Wallet → Balance**

* Shows **Eligible Balance**, **On Hold**, **Reserved**, **Net Available**, and **Next Payout ETA**.

**Cash Out Page (sub‑page)**

* **Payout summary:**
  + Gross donations eligible
  + Refunds (count/$)
  + Chargebacks (count/$)
  + Processing fees not covered (rare, see fees mode)
  + **Net available now**
  + Hold/reserve details
  + **Destination bank** (masked)
  + **Estimated arrival date**
* **Actions:**
  + **Request payout** (if eligible)
  + **Change destination**
  + **View statement PDF** (see 15.7)

**Post‑request states**

* **Requested** → **In Review** (risk/eligibility quick pass) → **Processing** (queued to bank) → **Paid** (settled)
* Failure paths: **Failed** (retry pending), **Returned** (bank rejected), **Canceled** (by Admin)

**AC**

* **AC‑CO‑1:** “Request payout” creates a Payout record with status **Requested** and a unique ID.
* **AC‑CO‑2:** Organizer gets email/SMS confirming the request with ETA.

**15.6 Statuses (badges & definitions)**

* **Not Eligible** — missing requirements (checklist shows which).
* **Hold** — within cooling‑off window; shows end‑date.
* **Eligible** — all requirements met; can Request Payout (or auto‑runs at next cycle).
* **Requested** — organizer triggered payout; queued for review.
* **In Review** — automated risk & compliance checks running.
* **Processing** — sent to bank; awaiting settlement.
* **Paid** — completed successfully; show arrival date.
* **Failed** — gateway error; will retry.
* **Returned** — bank rejected/returned (e.g., closed account); action required.
* **Compliance Hold** — trust or KYC review; donations frozen from payout.

**AC**

* **AC‑STS‑1:** Each status has a corresponding **color chip** (Gray/Yellow/Blue/Green/Red).
* **AC‑STS‑2:** Status changes trigger notifications (see 15.10) and write to an **Audit Log**.

**15.7 Statements & payout math**

**Organizer Statement (per payout)**

* **Header:** Campaign name, ID, date range, payout ID, destination bank (masked), payout date, payout amount.
* **Body:**
  + **Gross donations (eligible period)**
  + **Tips** (for the platform; **not** included in payout)
  + **Processing fees** (if not covered by donors)
  + **Cover‑fees collected** (offsets fees when donor opted in)
  + **Refunds** (issued within the period)
  + **Chargebacks** (initiated in period)
  + **Adjustments** (admin credits/debits)
  + **Reserve** (if any)
  + **Net to payout** (the transfer amount)

**Math (summary, consistent with Section 14 cover‑fees modes)**

* **Net to campaign per donation** =
  + If **Cover fees ON (donation‑only mode)**: approximately **donation amount** (½‑cent rounding may occur); platform receives tip.
  + If **Cover fees OFF**: **donation − fees**.
* **Payout amount** = Σ (eligible **Net to campaign**) − refunds − chargebacks − adjustments − **reserve**.

**AC**

* **AC‑STMT‑1:** Downloadable **PDF statement** per payout and **CSV** for the detailed line items.
* **AC‑STMT‑2:** Organizer can filter statements by campaign and date.

**15.8 Tax center (Organizer)**

**Individuals**

* **Tax profile wizard:** legal name, SSN last‑4, address confirmation.
* **Year‑end forms:** 1099‑K visibility **if applicable** (thresholds subject to IRS rules; copy will avoid numeric commitments and link to KB).
* **W‑9** attestation step when required (UI form; stored status).

**Organizations (EIN)**

* **Business profile:** legal name, EIN, business address; authorized representative attestation.
* **Year‑end reporting:** “We partner with our payments provider to deliver applicable tax forms. Thresholds and rules may change; see the KB.”

**AC**

* **AC‑TAX‑1:** Tax Center shows current profile status and past forms when available.
* **AC‑TAX‑2:** Missing tax data blocks payout with a checklist link to complete it.

**15.9 Failures, returns & negative balance**

**Failures/returns**

* If **Failed** (gateway error) → auto‑retry **daily for 5 days**; organizer gets a banner and can **Change destination**.
* If **Returned** (e.g., closed account) → payout is canceled; funds revert to campaign balance; organizer must update bank; **Request Payout** again.

**Negative balances**

* Causes: chargebacks or admin adjustments **after** payout.
* Handling:
  + Future eligible balances are **auto‑applied** to clear the negative first.
  + If balance remains negative for **>30 days** or exceeds **$1,000**, trigger **Finance Ops** workflow; organizer may be asked to **top up** or a repayment plan set.
  + Organizer portal shows **“Negative balance”** badge with explanation.

**AC**

* **AC‑NEG‑1:** Negative balances block new payouts until cleared.
* **AC‑NEG‑2:** Organizer is notified with steps to resolve.

**15.10 Notifications (Email/SMS/Portal)**

**Organizer**

* **Campaign ended** → “Hold until {date}” with checklist.
* **Eligible for payout** → “You can cash out now” (or auto‑payout ETA).
* **Payout requested** → confirmation with ID/ETA.
* **In Review** → only for manual checks >24h.
* **Processing** → date and destination.
* **Paid** → settled confirmation (with statement link).
* **Failed/Returned** → reason + CTA to update bank.
* **Compliance Hold** → high‑level reason, support link.

**Admin/Finance Ops**

* Large payout thresholds, mismatched names, repeated returns, negative balance >$1k, SLA breaches.

**AC**

* **AC‑NOTIF‑1:** All notifications are logged; deduped per status change.

**15.11 Organizer portal IA (Wallet)**

**Wallet → Balance (default)**

* Cards: **Eligible Balance**, **On Hold**, **Reserved**, **Net Available**, **Next Payout ETA**.
* Button: **Cash Out** (disabled with reasons if ineligible).

**Wallet → Cash Out**

* Payout summary, bank destination, “Request Payout”, “Change destination”, statement links.

**Wallet → Payout History**

* Table: Payout ID, date, amount, destination masked, status chip, actions (View statement, Download PDF/CSV).

**Wallet → Payout Destination**

* Current bank (masked), **Replace** flow (OTP + cooldown), change log.

**Wallet → Tax Center**

* Profile status; forms/history; links to KB.

**AC**

* **AC‑WAL‑1:** Replacing bank triggers cooldown; indicates when payout can resume.
* **AC‑WAL‑2:** Payout History supports search and date filters.

**15.12 Admin/ops controls**

**Admin Console → Payouts**

* Search by organizer, campaign, payout ID; filter by status.
* View payout detail: eligibility snapshot, risk score, holds/reserves, statement math, logs.
* Actions: put/release **Compliance Hold** (with reason), **Cancel** payout (before Processing), **Trigger retry**, **Override reserve**, **Force statement regenerate**.

**Finance Ops**

* **Returns queue**: see bank return codes; bulk notify organizers; quick link to change destination.
* **Negative balance**: aging list; contact log; repayment plans (notes only in MVP).

**AC**

* **AC‑ADMIN‑1:** All admin actions write to **Audit Log** with actor/time.

**15.13 Data model (conceptual)**

* **PayoutAccount**: user\_id/org\_id, bank\_masked, verified\_at, replaced\_at, status, name\_match\_flag.
* **Payout**: id, campaign\_id, user\_id (recipient), status, requested\_at, reviewed\_at, processed\_at, paid\_at, amount, destination\_ref, failure\_code, return\_code, eta\_date.
* **CampaignWallet**: campaign\_id, eligible\_balance, on\_hold, reserved, negative\_balance, last\_settlement\_run.
* **Statement**: payout\_id, summary fields (gross, tips, fees, refunds, chargebacks, reserve, net), pdf\_ref, csv\_ref.
* **AuditLog**: actor, action, target\_type/id, before/after, timestamp.

**15.14 Microcopy (ready for UI)**

* **Wallet banner (Hold):** “Your campaign ended on **{date}**. Funds will be available after a short review period ending **{hold\_date}**.”
* **Eligibility checklist item:** “Add a payout bank account to receive your funds.”
* **Request confirmation:** “We’re sending **${amount}** to your bank ending in **{last4}**. Estimated arrival **{eta}**.”
* **Failed/Returned:** “We couldn’t deliver your payout. Reason: **{code/description}**. Please update your bank details to try again.”
* **Negative balance:** “Your campaign wallet is negative by **${amount}** due to recent disputes/refunds. New payouts are paused until this is resolved.”

**15.15 Acceptance criteria summary (engine‑ready)**

* Payouts run **after campaign end** + **3–5 business day hold**; **auto‑payout** if eligible; manual **Request Payout** also available.
* **Eligibility:** ID verified, SSN/EIN profile complete, verified bank, min $50, no holds.
* **Destination:** one active bank; OTP on change; 24‑hour cooldown; name mismatch → Compliance Hold.
* **Statuses:** Not Eligible, Hold, Eligible, Requested, In Review, Processing, Paid, Failed, Returned, Compliance Hold.
* **Failures:** retry daily ×5; Returned returns funds to balance; organizer notified.
* **Negative balances:** block payouts; auto‑apply future funds; escalate >$1k or 30 days.
* **Statements:** PDF + CSV with full math; per‑payout; downloadable.
* **Notifications:** comprehensive organizer/Admin triggers.
* **Admin:** search, view, holds, cancel, retry, override reserve; full audit.

**15.16 Optional & Phase‑2 ideas (not in MVP, for roadmap)**

* **Instant Payouts** to debit cards for a small fee (faster settlement).
* **Multiple payout schedules** (weekly vs on‑demand) per organizer preference.
* **Partial payouts** mid‑campaign (still keep end‑of‑campaign default).
* **Repayment plans** tooling (for negative balances).
* **Granular reserves** rules engine (auto holds based on risk signals).

**15.17 Open items**

* **Exact hold length display**: I’ll display a concrete date based on a **5 business‑day** default; we can tune to **3–5** operationally.
* **Reserve policy:** default **0%**; Admin can set case‑by‑case.
* **Fees coverage mode:** set to **donation‑only** for the “cover fees” gross‑up (Section 14 math)

## Small additions to Section 15

1. **Large‑payout re‑auth**
   * If **payout request ≥ $10,000**, require an extra **SMS OTP** at request time (in addition to any cooldown on bank changes).
   * Reason: protects against account takeover in high‑value cases.
   * **AC‑SEC‑1:** Requests ≥ $10k log a successful OTP step in Audit Log.
2. **Cutoff & ETA clarity**
   * Display a daily **payout run cutoff** (e.g., **5:00 PM ET**) and a calculated **ETA** that accounts for US bank holidays.
   * **AC‑ETA‑1:** Cash Out page shows “Requested before 5:00 PM ET → estimated arrival **{date}**.”
3. **Returned‑payout fast lane**
   * If a payout is **Returned**, after the organizer updates bank details, show a **“Resubmit now”** button (doesn’t wait for the next automatic cycle).
   * **AC‑RET‑1:** Clicking “Resubmit” creates a new payout with reference to the returned one.
4. **Statement scope line**
   * Each statement includes a “**Donations included through {timestamp}**” line so organizers understand the accounting window.
   * **AC‑STMT‑3:** Timestamp reflects campaign end (local time) and any refunds applied before payout processing.

# 

# 

# Section 16 — Public Website & Discovery

**16.0 Scope & dependencies**

**Scope:** Home, Search, Category/Tag/Location listings, Result cards, “Related campaigns,” public entity profiles entry points, SEO (meta/OG/JSON‑LD), sitemaps, indexing & ranking, personalization (lightweight), accessibility & performance budgets, analytics, and admin curation hooks.  
**Depends on:** Section 12 (taxonomy, campaign page), Section 10 (public entity profiles, DM rules), Section 20 (CMS, curation, ranking knobs), Section 18 (share/OG), Section 11 (badges).

**16.1 URL architecture & routing**

* **Home:** /
* **Search:** /search?q={query}&category={slug}&state={us-state}&status={live|ended}&funding={aon|kwr}&min={int}&max={int}&near={lat,lon}&sort={relevance|trending|new|ending|most\_raised|most\_donors|near\_me}
* **Category:** /category/{slug}
* **Tag:** /tag/{slug}
* **Location:** /us/{state}/{city?} (optional city)
* **Campaign:** /c/{slug}-{id} (stable ID to avoid slug collisions)
* **Public user:** /u/{username}; **Org:** /org/{org\_slug}; **Team:** /team/{campaign\_slug} (from §10.T)
* **Error/Status:** /suspended, /not-found (SEO‑friendly copy)

**AC‑URL‑1:** All filters/sort/pagination persist in query params (shareable, indexable where appropriate).  
**AC‑URL‑2:** 301 legacy redirects handled by Admin (20.P Redirects).

**16.2 Home (discovery hub)**

**Modules (reorderable via Admin CMS 20.O):**

1. **Hero**: headline, subhead, primary CTA (“Start a campaign”), secondary CTA (“Browse campaigns”).
2. **Trending now** (data‑driven): top 6 campaigns.
3. **Editor’s Picks** (curated): 4–8 handpicked.
4. **Ending soon**: 6 ending within 72 hours.
5. **In your state**: geolocate (consent) or IP→state fallback.
6. **Categories**: 12 primary categories (from §12.A.1) with icons.
7. **Verified nonprofits**: strip showing orgs with EIN+IRS badge.
8. **Recently launched**: newest 6.
9. **Knowledge & safety**: links to policies/KB.

**AC‑HOME‑1:** Each module lazy‑loads; LCP element is Hero or first card in Trending.  
**AC‑HOME‑2:** Geolocation prompt is optional; decline → show US defaults (e.g., national mix).  
**AC‑HOME‑3:** “Feature on homepage” and “Pin to category” reflect Admin actions (20.F.27).

**16.3 Category, Tag & Location pages**

**Header:** title, brief description, facet summary (“1,245 campaigns in Medical & Health”).  
**Facets:** Category (pre‑selected), Tags (multi), State, City (state‑scoped), Funding model (KWR/AoN), Status (Live/Ended), Verified (User/Org), Nonprofit badge, Team enabled, Goal range, Raised range, % Funded buckets (0‑25/25‑50/50‑75/75‑100/100+), Days left buckets.  
**Sort:** Relevance (if query), Trending, Newest, Ending soon, Most raised, Most donors, Near me (if location known).  
**Empty state:** “No matches—try removing filters or searching related terms.”

**AC‑CAT‑1:** Facets reflect counts; selecting State limits City list.  
**AC‑CAT‑2:** “Clear all” resets facets while preserving page context.

**16.4 Search UX (site‑wide)**

**A) Search box & typeahead**

* Autocomplete suggestions: campaigns (title+thumb), categories, tags, states/cities.
* “Did you mean” for typos; basic synonyms (e.g., *memorial ↔ funeral*, *hurricane ↔ storm*).
* Recent searches (client‑side, private).

**B) Results**

* Left rail: facets (as above).
* Main: result grid 3‑up desktop / 2‑up tablet / 1‑up mobile (skeleton loaders).
* Zero results: show relaxing filters + related categories/tags; offer Support link.

**C) Query handling**

* Phrase match for quotes; stemming/plurals; typo tolerance (1 edit distance for words ≥5 chars).
* Boosts: title > tags > short\_desc; de‑boost suspended/ended by default unless “Ended” facet is on.

**AC‑SRCH‑1:** Query string always reflects current filters & sort.  
**AC‑SRCH‑2:** Results exclude Suspended/Removed; Ended hidden unless explicitly included.  
**AC‑SRCH‑3:** “Report this campaign” is donors‑only: show sign‑in CTA otherwise.

**16.5 Campaign card (listing component spec)**

**Required fields:**

* Cover image (16:9, lazy‑loaded, alt from media alt text)
* Title (2‑line clamp)
* Organizer display name (clickable to profile) + **verified badge** + **nonprofit badge** (if any)
* Category & city/state
* Progress bar + **$ raised** / **goal** + **% funded**
* **Days left** (or “Ended {date}”)
* **Donate** button (primary), **Share** (secondary)

**Optional chips:** “Editor’s Pick”, “Trending”, “Ending Soon”, “Team Fundraiser”.

**States:**

* **AoN not funded (ended)**: show “Not funded—auto‑refunded” badge; Donate disabled.
* **Suspended**: do not show card (removed from discovery).
* **Overfunded**: show “100%+ funded” chip.

**AC‑CARD‑1:** Card accessible: semantic heading, proper alt, buttons keyboard focusable.  
**AC‑CARD‑2:** CTA opens campaign page with #donate anchor on mobile.

**16.6 “Related campaigns” (on campaign page)**

**Logic:**

* Match on **category** + **top tags** + **state proximity**; exclude the current campaign.
* Mix 6 items: 4 algorithmic + 2 curated if available.

**AC‑REL‑1:** Never surface Suspended/Removed; respect nonprofit badge filters if present.  
**AC‑REL‑2:** For AoN ended not funded, still show related (discovery continues).

**16.7 Public entity profiles in discovery**

* All organizer/org/team names on cards and pages are **clickable** (from §10.T).
* Profiles include **Message** CTA (honors DM policy: Anyone / Donors‑only / Off).
* Listings from a profile (their campaigns) inherit same card component.

**AC‑PROF‑1:** If entity hides certain stats (10.T settings), omit those panels gracefully.  
**AC‑PROF‑2:** DM button opens login/signup when not authenticated.

**16.8 Ranking & “Trending” algorithm (user‑facing + admin overrides)**

**Signals (weights are Admin‑tunable in 20.P):**

* **Text relevance (if query)** — title (x3), tags (x2), short\_desc (x1)
* **Freshness** — recency of launch and updates
* **Velocity** — donations per hour (last 24–72h) with decay
* **Engagement** — visitors→donations conversion rate (min traffic threshold)
* **Progress** — % funded (cap boost near 90% to prevent runaway dominance)
* **Badges** — verified user/org (+ small boost), verified nonprofit (+ small boost)
* **Curation** — Editor’s Pick (+ controllable boost)
* **Quality** — media completeness (cover present, story length above minimum)

**Fairness & safety rails**

* Capped boosts to avoid single‑factor dominance; no personalization that would hide safety‑critical content.
* Suspended/Removed = rank 0 (not shown).
* **Disclosure**: Where “Editor’s Pick” or curation override applies, card shows the chip.

**AC‑RANK‑1:** Changing weights in Admin shows live **simulation** before apply (20.P).  
**AC‑RANK‑2:** Trending list updates at least every **15 minutes**.

**16.9 Personalization & location (lightweight)**

* **“In your state”** module uses state‑level IP or consented geolocation.
* **“For you” (Phase‑2):** Optional section for logged‑in users blending their viewed categories and campaigns with platform popularity; opt‑out available.

**AC‑LOC‑1:** Declining location prompts does not degrade core discovery; show national defaults.

**16.10 SEO & share**

**Technical SEO**

* **SSR/SSG** for all public pages; canonical URLs; unique titles & meta descriptions; clean slugs.
* **Robots:** allow public pages; disallow /portal/\*, /admin/\*, /api/\*.
* **Sitemaps:**
  + sitemap.xml index → sitemap-campaigns-N.xml (rotating sets), sitemap-categories.xml, sitemap-profiles.xml.
  + Update **daily**; new/updated campaigns prioritized.

**Structured data (JSON‑LD)**

* WebSite with SearchAction (site search).
* CollectionPage for category/tag pages.
* Organization / CharitableOrganization for verified org profiles.
* CreativeWork (or Project) for campaign pages: name, description, image, creator (Organization/Person), location, startDate, endDate, isAccessibleForFree: true.
* BreadcrumbList on campaign and category pages.

**OpenGraph/Twitter**

* OG title: {Campaign Title} | {Brand}
* OG description: short\_desc; add AoN note if applicable.
* OG image: generated via Admin OG template (20.O) with overlay and progress bar toggle.

**AC‑SEO‑1:** Canonical tags present; paginated results carry rel prev/next.  
**AC‑SEO‑2:** Suspended/Removed return **410** or **noindex** (Admin policy toggle).  
**AC‑SEO‑3:** AoN not funded: page remains indexable with clear status.

**16.11 Compliance, moderation & delisting policy**

* **Suspended** campaigns hidden from discovery/search; direct URL shows “Temporarily unavailable due to review” (public, donations disabled).
* **Removed** campaigns return 410; show helpful “Campaign not available” page with links to browse/search.
* **Reported (not actioned)** campaigns remain visible (donors‑only reporting; 20.B drives moderation).

**AC‑COMP‑1:** Discovery always respects moderation states from Admin.

**16.12 Accessibility & performance budgets**

* **Budgets (desktop over 4G):**
  + LCP ≤ **2.5s** (hero or first card), CLS ≤ **0.1**, TBT ≤ **200ms**.
* **Images:** responsive sizes, srcset, lazy‑load offscreen, WebP/AVIF where supported; meaningful alt.
* **Keyboard:** facet controls tabbable, ARIA for accordions, skip‑to‑content link.
* **Color/contrast:** chips and progress bars meet WCAG 2.2 AA.

**AC‑PERF‑1:** Lighthouse ≥ 90 Performance/Accessibility on Home, Category, Search, Campaign.

**16.13 Analytics & telemetry**

* **Search analytics:** queries, zero‑result rate, CTR by position, facet usage, abandonment, time to first result.
* **Listing analytics:** module CTRs (Trending, Ending), card hover→click rates, add‑to‑donate CTR.
* **SEO analytics:** impressions, clicks, average position per page type.
* **Attribution:** UTMs propagated to campaign page and checkout; member referral codes preserved through navigation (12.J.3).

**AC‑ANL‑1:** Cookie‑lite approach for anonymous users; comply with privacy laws; do not store PII without consent.

**16.14 Admin controls mapping (20.O/20.P)**

* **CMS (20.O):** reorder Home modules; edit copy; schedule variants; OG template editor.
* **Discovery (20.P):** feature/pin campaigns; ranking weights; synonyms; stop‑words; typo tolerance; redirects & canonicals; search facet configuration; simulation UI.
* **Experiments (20.Q):** donation presets exposure, facet ordering, module visibility A/B.
* **Config (20.I):** default sort, “Ended” visibility, “Ending soon” window, image size caps.

**16.15 Indexing & data model (conceptual)**

* **SearchIndexCampaign**: campaign\_id, title, short\_desc, story\_excerpt, category, tags[], city, state, status, funding\_model, verified\_user, verified\_org, nonprofit\_verified, goal, raised, pct\_funded, donors\_count, start\_date, end\_date, last\_update\_at, donation\_velocity\_24h, editors\_pick, team\_enabled, popularity\_score
* **SearchIndexProfile**: user/org/team fields for autocomplete.
* **SynonymSet**: admin‑managed pairs/groups.
* **RankingConfig**: weights for signals; decay half‑life; caps.

**Indexer**

* Triggers on campaign publish/update/new donation/refund/moderation changes; recompute velocity and popularity; push to index within **< 2 minutes**.

**AC‑IDX‑1:** Index reflects new donations in Trending within **15 minutes** (batch window).

**16.16 Acceptance Criteria (summary)**

* **Home** shows configurable modules; geolocation optional; Accessible & fast.
* **Search & Listings**: full facet set; persistent URL; zero‑result assistance; suspended hidden; ended opt‑in.
* **Cards**: consistent, accessible, correct chips/badges; Donate CTA deep‑links.
* **Related**: 6 mixed items; excludes suspended; includes curated when available.
* **Profiles**: all name links route to correct public profile; DM CTA respects policies.
* **Ranking**: admin‑tunable signals with simulation; refresh cadence met; safety rails enforced.
* **SEO**: canonical/OG/JSON‑LD; sitemaps daily; correct robot rules and 410/noindex policies.
* **Perf/Access**: budgets met; images optimized; keyboard/ARIA complete.
* **Analytics**: search & listing telemetry captured; UTMs/ref codes preserved.
* **Indexing**: donation velocity reflected rapidly; moderation updates propagate.

**16.17 Microcopy (ready to ship)**

* **Search placeholder:** “Search campaigns, categories, or locations”
* **Zero results:** “No matches found. Try different keywords or remove some filters.”
* **Trending chip tooltip:** “Rising support in the last few days”
* **Editor’s Pick chip:** “Featured by our team”
* **Ending soon chip:** “Less than 72 hours left”
* **Suspended page:** “This campaign is temporarily unavailable while we review a report.”
* **Not funded (AoN):** “This all‑or‑nothing campaign didn’t meet its goal. All donations were refunded.”

**16.18 Roadmap & experiments**

* **Personalized “For you”** shelf with clear opt‑out.
* **Location clustering** down to city/zip (privacy‑safe).
* **Advanced synonyms** with ML (semantic search) while keeping deterministic fallbacks.
* **Infinite scroll vs. pagination** A/B on Search.
* **“Follow organizer”** to receive update notifications (ties into §18).
* **Accessibility enhancements**: prefers‑reduced‑motion animations for progress bars.

# Section 16B — Search & Discovery

**Scope:** Global search, category browsing, discovery rails on Home, ranking formulas (relevance/trending/freshness), facets & sort options, typeahead, SEO for lists, a11y & performance budgets, anti‑gaming safeguards, admin tuning & editorial controls, analytics, data bindings, acceptance criteria, and QA.

**Depends on:** §0 (US‑only policies), §4 (UX/A11y/Perf), §5 (Risk & Abuse), §6 (Privacy/Legal), §7 (APIs), §8 (DB & index projections), §9 (CMS/editorial), §10 (Portal UI), §11 (KYC), §12–15 (Campaign lifecycle), §18 (Notifications), §20 (Admin), §21–22 (Ops/QA).

## 16.0 Principles

* **Findability first:** the right campaign, fast.
* **Trust by design:** verified badges and policy‑compliant visibility; explainable ranking.
* **Fast on mobile:** SSR for above‑the‑fold list, LCP ≤ 2.5s, keyboardable facets.
* **Fair & abuse‑resistant:** no keyword spam or dupes dominating results.
* **Privacy:** respect donor anonymity and organizer privacy rules; show only public data.

## 16.1 Surfaces & routes

* **Global Search page:** /search?q=…&filters…
* **Categories:** /discover/{category-slug} (e.g., /discover/medical)
* **State filters:** /discover/us/{state} (e.g., /discover/us/ca)
* **Home discovery rails** (modules in §16.10) with deep links into search presets.
* **Typeahead** (header search) with instant suggestions (campaigns + categories + tags).
* **SEO:** canonical for each filter/sort combination (see §16.12).

## 16.2 Result card (unified across lists)

Each card (same as Section 13 list card):

* **Cover thumbnail** (16:9, lazy) with **Verified**/**Nonprofit** badges overlay chips.
* **Title** → campaign page; **Category chip**; **City, ST**; **KWR/AoN** chip.
* **Progress bar** with “$X of $Goal • Y days left” (supports **Ended**/**Not funded** states with gray/red chips).
* **Team enabled** indicator (optional icon).
* **A11y:** card is a <article>; title is <h2>, alt text on image; progress has aria-valuenow.

## 16.3 Facets & filters (left rail / top on mobile)

**Default facets (MVP):**

1. **Category** (12 primary categories from §12.A.1). (multi-select)
2. **Location**
   * **State** (US states; multi-select)
   * **City** (dependent on state; multi-select; top 20 by freq when state selected)
3. **Funding model**: KWR, AoN.
4. **Verification**
   * **Organizer verified** (ID+phone+email, the 4/4 badge)
   * **Verified Nonprofit** (EIN matched)
5. **Campaign status**: Live (default), Ended, Not Funded (off by default).
6. **Has rewards**: yes/no.
7. **Media**: Has video.
8. **Last updated**: Past 24h / 7d / 30d.
9. **Team fundraising**: Enabled.

**Filter logic:** AND within a facet group when multi‑select?

* **Within a single facet**: **OR** (e.g., Category A OR B).
* **Across different facets**: **AND**.

**A11y:** Each facet is a fieldset with legend; checkboxes with labels; “Clear all” button & per‑facet “Clear”.

## 16.4 Sort options

* **Relevance (default for keyword queries)**
* **Trending** (time‑decayed donations velocity; see §16.7)
* **Newest** (by start\_date DESC)
* **Ending soon** (by end\_date ASC, Live only)
* **Most supporters** (unique donors count DESC)
* **Most raised** (amount raised DESC; KWR & funded AoN only)

**Guardrails:** “Most raised” excludes AoN **not funded**; “Ending soon” hides ended.

## 16.5 Query parsing & typeahead

### 16.5.1 Query parser (MVP)

* **Free text** over **title** (boost 5×), **tags** (4×), **category name** (2×), **story** (1×), **FAQ** (0.5×), **city/state** (1×).
* **Operators** (simple):
  + Phrase with quotes: "brain surgery"
  + Field filters: category:medical, state:CA, city:"San Diego", aon:true, rewards:true, nonprofit:true, updated:<7d, ends:<14d.
* **Typo tolerance** (1 edit distance for tokens ≥ 5 chars) with **did‑you‑mean** suggestion if top 3 results score low.
* **Synonyms (seed list)**:
  + memorial ↔ funeral, hurricane ↔ storm, tuition ↔ school fees, animal ↔ pet, startup ↔ small business, church ↔ ministry, soccer ↔ football (US).
  + Managed in Admin (20.I → Search config).

### 16.5.2 Typeahead (header search)

* **2 columns:**
  + **Campaigns (top 5)**: title + location + category chip.
  + **Browse**: the 12 categories + most popular tags (top 5).
* Keyboard arrows navigate; Enter opens result; Esc closes.
* Server returns <200ms P95 from warm cache.

## 16.6 Indexing, freshness & infra

* **Index store:** OpenSearch/Elasticsearch or similar (managed), campaign\_index\_v{n}.
* **Document schema:**
* id, title\_text, tags[], category, story\_text, faq\_text,
* city, state, location\_text, is\_live, is\_aon, is\_verified\_organizer, is\_verified\_nonprofit,
* has\_rewards, has\_video, team\_enabled,
* start\_date, end\_date, last\_update\_at,
* amounts: { raised\_cents, goal\_cents, supporters\_count },
* trending: { score\_1h, score\_24h, score\_7d, last\_recalc\_at }
* **Pipelines:**
  + **On publish/unpublish/suspend** → upsert/remove doc within **< 10s**.
  + **On donation/refund/dispute** → update amounts and trending counters within **≤ 60s** (via event consumer).
  + **Nightly** reindex for drift; alias swap with zero downtime.
* **Text analysis:** English analyzer with stemming; custom stopwords; synonyms filter.
* **Safety:** never index **suspended** or **unpublished**; ended/not‑funded doc stays but “Live only” filter hides by default.

## 16.7 Ranking formulas (explainable)

### 16.7.1 Relevance (BM25 + field boosts)

* **Score = BM25(title×5 + tags×4 + category×2 + story×1 + faq×0.5 + city/state×1)**
* Plus **recency boost** for last\_update\_at (≤7d → +5%; ≤24h → +10%).
* **Verified boost:**
  + Organizer verified: × **1.05**
  + Verified Nonprofit: × **1.10**
* **Result explainability:** Admin can view top features for a query in debug (20.I).

### 16.7.2 Trending (decayed velocity; Live only)

**Intuition:** more supporters and dollars in the recent window → higher rank, decayed by time.

* **Inputs (windowed):**
  + donations\_24h\_count, donations\_24h\_amount
  + donations\_7d\_count, donations\_7d\_amount
* **Score:**
* S\_trend =
* w1 \* log1p(donations\_24h\_amount) +
* w2 \* donations\_24h\_count +
* w3 \* log1p(donations\_7d\_amount) +
* w4 \* donations\_7d\_count
* **Default weights (Admin‑tunable):** w1=0.70, w2=0.30, w3=0.25, w4=0.10.
* **Category normalization:** divide by median(S\_trend) within category to avoid one category dominating.
* **Freshness decay:** multiply by exp(-age\_hours / τ) with τ=48h.
* **Badges:** Verified Nonprofit × **1.05** post‑score.

### 16.7.3 Ending soon (Live only)

* Rank by end\_date ASC, break ties by percent\_to\_goal DESC.

### 16.7.4 Most supporters / Most raised

* Pure sort by supporters\_count or raised\_cents (ties → recency).
* **Guardrail:** “Most raised” excludes AoN not‑funded and suspended.

## 16.8 Abuse & anti‑gaming

* **Keyword stuffing:** detect high tf/idf mismatch (title with >8 repeated keywords) → **score penalty** ×0.8; show in Admin “Quality Issues”.
* **Duplicate detection:** near‑duplicate shingling (title+story) → cluster; only one shows for a query; others demoted unless filtered by location.
* **Velocity manipulation:** bursts with same BIN/IP → risk engine tags suspicious\_velocity; **Trending** penalized ×0.7 until cleared.
* **Exact‑match domain hijack:** strip tracking/URLs from stories; ignore link text in scoring.
* **Policy enforcement:** suspended campaigns removed from index; “Under review” set to **paused** (hidden from Trending/Ending Soon rails, visible only in direct URL).

## 16.9 Pagination, performance & a11y

* **Page size:** 24 results (desktop), 18 (mobile).
* **Pagination:** numbered (SEO‑friendly) + rel="prev/next". Infinite scroll optional toggle (Phase‑2).
* **Skeleton loaders** while new page loads.
* **Performance budgets (per §4.6 Search/Category row):** LCP ≤ **2.5s**, CLS ≤ **0.10**, TBT ≤ **200ms**, JS ≤ **180KB** gz.
* **A11y:**
  + Search input labelled; aria-live="polite" for result count updates.
  + Facets are groups with legends; keyboardable; “Apply filters” button on mobile.
  + Announce “X results for {query}” in SR only region.

## 16.10 Home discovery rails (config & ranking)

Modules (order configurable in CMS §9; defaults below):

1. **Trending near you** (if we can infer state)
   * Filter: state = viewer\_state (fallback to national).
   * Sort: **Trending**.
   * 8 cards.
2. **Editor’s Picks** (CMS curated)
   * Up to 8 pinned campaigns (manual pick, expires after N days).
   * Always appear first; remaining slots backfilled by **Relevance** to a curated tag (“editors-pick”).
3. **Ending soon**
   * Live, end\_date ≤ 7 days, sort “Ending soon”.
   * 8 cards.
4. **New & noteworthy**
   * Published ≤ 7 days, with at least one donation (to avoid empty).
   * Sort by raised\_cents DESC then last\_update\_at DESC.
   * 8 cards.
5. **Verified nonprofits**
   * is\_verified\_nonprofit = true, sort by **Trending**; 8 cards.
6. **By category** carousels (Medical, Community, Education...)
   * Each is a deep link to /discover/{category} with top 6.

**A/B hooks:** order of rails, card count, localization copy. Must honor §4 budgets.

## 16.11 No‑results & query assistance

* **Zero state:** “We couldn’t find anything for **‘{q}’**.”
  + Suggestions: check spelling; try synonyms; broaden filters; browse categories.
  + Show **popular categories** chips + **Editor’s Picks** fallback rail.
* **Did‑you‑mean**: offer single correction if Levenshtein edit distance 1–2 increases estimated matches ≥ 5×.
* **Spell correction opt‑out:** keep original query accessible via link “Search instead for ‘{original}’”.

## 16.12 SEO for lists

* **Title/Meta:** include query or category and state (e.g., “Medical fundraisers in California | {brand}”).
* **Canonical:**
  + /discover/{category} canonicalizes to itself.
  + /search?q=… canonicalizes to itself **only** when filters are applied; otherwise canonical to base /search.
* **Robots:** allow crawl on list pages; **noindex** on pages with zero results or with deep pagination beyond page 10 to reduce thin content.
* **Structured data:** CollectionPage with itemListElement of campaign URLs (top 10 per page).

## 16.13 Admin controls (Search & Discovery console, §20.I)

* **Weights:** sliders for relevance boosts (title/tags/story/faq), verified boosts, trending weights (w1..w4), decay τ.
* **Synonyms manager:** add/edit/delete; import CSV.
* **Pinner:** UI to **pin** campaigns to specific rails or categories with **start/end dates**; drag to order.
* **Boost/demote:** manual ± boosts on a campaign (±10%, ±25%, ±50%) with expiry.
* **Quality monitor:** list campaigns with keyword stuffing/duplicate risk flags; one‑click “require edits” (20.B).
* **Region rules:** ability to disable “Near you” rail if no state can be inferred reliably.
* **Experiment toggles:** choose rail order for A/B variants; sampling ratio.
* **Audit:** every change recorded in admin.audit\_log.

## 16.14 Analytics & KPIs

**Events (front‑end):**

* search\_page\_view{q, facets, sort}
* search\_execute{q\_len, facet\_count, result\_count}
* search\_result\_click{position, campaign\_id}
* facet\_toggle{name, value, on\_off}
* sort\_change{to}
* typeahead\_select{type:campaign|category|tag, id}
* rail\_view{name} / rail\_card\_click{name, position, campaign\_id}

**KPIs:**

* **Search → donate** funnel conversion.
* **CTR** on top rail cards; **dwell time** on category pages.
* **No‑result rate**, **spell‑assist CTR**.
* **Diversity index** (category distribution on Home rails).
* **Freshness**: avg age of items on Trending.
* **Abuse**: campaigns with stuffing/dup flags per 1k indexed.

## 16.15 Data model & indexes (ties to §8)

**New / updated projections:**

* search.campaign\_projection (materialized view or ETL) with fields in §16.6.
* search.synonyms {term, synonyms[], active, updated\_at}.
* search.quality\_flag {campaign\_id, reason('stuffing'|'duplicate'|'velocity\_anomaly'), weight, detected\_at}.
* **Counters** tables (for trending windows) updated by donation events.
  + agg.campaign\_donations\_hourly {campaign\_id, hour, count, amount\_cents}
  + agg.campaign\_donations\_daily {campaign\_id, day, count, amount\_cents}

**Indexes:** DB indexes to support ETL queries; OpenSearch/ES handles search indexes.

## 16.16 Acceptance Criteria (summary)

1. **Search page** renders quickly; result cards show correct badges, progress, and states.
2. **Facets & sort** work with AND/OR logic as specified; mobile “Apply filters” flow behaves.
3. **Typeahead** returns relevant suggestions in < 200ms warm; keyboardable.
4. **Relevance** honors field boosts and recency; **Trending** ranks by decayed velocity with category normalization.
5. **Ending soon, Most supporters, Most raised** sorts are correct and obey guardrails.
6. **Abuse controls** penalize stuffing and near duplicates; suspended campaigns are removed.
7. **Index freshness**: publish/unpublish/suspend visible ≤ 10s; donation counters ≤ 60s.
8. **Home rails** populate per spec; “Near you” respects state; fallbacks when empty.
9. **No results** experience provides help and suggestions; “did‑you‑mean” works.
10. **SEO**: canonical tags correct; noindex rules applied; structured data valid.
11. **A11y & Perf**: meets §4 budgets; SR announcements on counts; keyboard flows pass.
12. **Admin controls** can pin/boost and adjust weights with audit; changes reflected within 5 minutes.
13. **Analytics** events collected; dashboards show funnel & CTRs.

## 16.17 QA checklist (tie to §22)

* Keyword search with typos → correction suggestion; results sensible; “Search instead for …” present.
* Phrase query "medical bill" narrows correctly.
* Facet combinations (Category + State + Has rewards + Verified nonprofit) filter accurately.
* Sort toggles (Relevance/Trending/Ending soon/Most supporters/Most raised) reorder as expected.
* Publish/suspend/goal change propagate to list within SLA; ended/AoN not‑funded states appear with correct chips.
* Trending list changes after injecting donations; time decay verified via test harness.
* Near‑duplicate campaigns → only one prominent; others demoted.
* Keyword stuffing penalty: flagged in Admin; demotion visible.
* Typeahead: campaign pick navigates; category pick goes to category page.
* Home rails: empty edge cases (no near‑you; no ending soon) show fallback rails.
* A11y: SR announces “X results for …”; facets and cards keyboardable; focus management correct.
* Perf: Lighthouse budgets met; list pages render ≤2.5s LCP on mid mobile.
* Analytics events firing with expected payloads.

## 16.18 Microcopy kit (ready to ship)

* **Search input placeholder:** “Search fundraisers (title, category, city…)”
* **Results count:** “**{n}** results for **‘{q}’**” / “**{n}** {category} fundraisers in **{state}**”
* **No results headline:** “No fundraisers found for **‘{q}’**”
* **No results help:** “Try different keywords, remove some filters, or browse categories.”
* **Did‑you‑mean:** “Did you mean **{suggestion}**?”
* **Facet headers:** “Categories”, “Location”, “Funding model”, “Verification”, “Rewards”, “Media”, “Last updated”, “Team fundraising”
* **Clear filters:** “Clear all filters”
* **Trending rail title:** “Trending near you” / fallback “Trending now across the US”
* **Ending soon rail title:** “Ending soon”
* **New & noteworthy rail title:** “New & noteworthy”
* **Verified nonprofits rail title:** “Verified nonprofits”

## 16.19 Roadmap (Phase‑2)

* **Personalized discovery** (opt‑in): weigh past support categories & locations.
* **“Follow” campaigns** with update digests; **saved searches** with alerts.
* **Map view** for state/city discovery; geospatial boosts.
* **Advanced query operators** (min\_supporters:, percent\_to\_goal:, published:<30d).
* **Auto‑learn synonyms** from query logs; ML reranking.
* **Infinite scroll** with proper SEO hydration and load more fallback.

# Section 17 — Direct Messaging (DM) & Conversations

**Scope:** Private, in‑portal messaging across the product: donors ↔ organizers, donors ↔ orgs, donors ↔ teams (policy‑gated), reward‑context conversations, organizer shared inbox with role scoping, notifications, abuse controls, storage/retention, and admin tooling.  
**Depends on:** §3 (Roles & permissions), §4 (UX/A11y budgets), §5 (Risk & Abuse), §6 (Privacy & Retention), §7 (APIs & webhooks), §8 (DB), §10 (Portal), §12 (Rewards), §18 (Notifications), §20 (Admin), §21–22 (Ops/QA).

**Intent alignment:** You asked for **messaging on every entity profile** (user/org/team) **and** a **reward‑only** path. This spec delivers **both**:  
• **General DMs** (policy‑gated: Anyone / Donors‑only / Off) and  
• **Reward DMs** (contextual to a donation/tier; privacy‑protected).

## 17.0 Objectives & non‑goals

**Objectives**

1. Enable safe 1:1 coordination (reward shipping, clarifications) without exposing emails or phone numbers.
2. Provide organizers a **shared inbox** with role‑scoped access (Lead/Co‑Lead/Support).
3. Keep abuse low via **rate limits**, **report/block**, and **moderation cases**.
4. Keep performance and a11y at our global standard.

**Non‑goals (MVP)**

* No group chats beyond organizer‑side shared inbox.
* No email bridging (send/receive via email) or push notifications—**Phase‑2**.
* No end‑to‑end encryption (we store messages for safety/moderation; see §6).

## 17.1 Policies, roles & permissions

### 17.1.1 Entity‑level DM policy (configurable by each entity)

* **Anyone** (default) — any registered user can start a DM.
* **Donors‑only** — only users who have **donated to any campaign** can start.
* **Off** — cannot start new DMs; existing threads readable but locked.

**Organizer defaults:** General DMs = **Anyone**; Reward DMs = **Always ON** (cannot be disabled while rewards exist).  
**Org (nonprofit) defaults:** **Donors‑only** for general; **Always ON** for reward.

### 17.1.2 Thread visibility by role (campaign‑context)

| **Role** | **Can view general threads to the campaign?** | **Reward‑context threads?** | **Can reply as campaign?** |
| --- | --- | --- | --- |
| Organizer (Lead) | ✅ | ✅ | ✅ |
| Co‑Lead | ✅ | ✅ | ✅ |
| Campaign Support | ❌ | ✅ | ✅ (reward threads only) |
| Team Member | ❌ | ❌ | ❌ (personal DMs only; not on behalf of campaign) |
| Org Admin (nonprofit) | ✅ (all org campaigns) | ✅ | ✅ (audited) |
| Moderator / Staff | Read‑only (with justification) | Read‑only | ❌ |

**COI privacy:** Team Members cannot access donor reward details. Support cannot initiate outbound DMs to donors; **reply‑only** within reward context.

### 17.1.3 Donor privacy rules

* Donor **email/phone never shown** in DM.
* Donor may set **“Hide name publicly”** and still use DM; organizer sees display name only.
* **Anonymous donors** cannot DM the organizer about that donation (no identity to attach).

## 17.2 UX: entry points & flows

### 17.2.1 Where users start DMs

* **Entity profile pages** (user/org/team): **Message** button (policy‑gated).
* **Campaign page → Organizer card**: **Message organizer**.
* **Rewards → Donation detail**: **Contact organizer about this reward** (preloads **campaign\_id**, **donation\_id**, **tier\_id**).
* **Inbox** icon in portal header (with unread count).

### 17.2.2 Message composer (MVP)

* Plain text (max **2,000 chars**), emoji, **up to 2 links**, **profanity/harassment filter** (soft warn).
* Attachments: **images only** (jpg/png/webp), **≤3 files**, **≤5 MB each**; previews in composer; optional **caption** (a11y).
* **No HTML**; links auto‑linkified; no inline iframes.
* **Send** on Enter (Shift+Enter for newline).

### 17.2.3 Inbox & thread UI

* **Left rail**: Threads list (unread first), search by name/campaign, filters: All / Reward / Archived.
* **Right pane**: Conversation; header shows **participants + context**; actions: **Mute**, **Report**, **Block** (entity), **Archive**, **Mark unread**.
* **Tombstones**: “Message deleted by sender” when within edit window (see §17.8).
* **A11y:** list items are buttons/links; threads labeled with unread counts; live region for “New message received”.

## 17.3 Delivery architecture & performance

* **Transport:** HTTPS API + **WebSocket** channel (/ws/messages) for live updates; **SSE** fallback; **long‑polling** final fallback.
* **Auth:** JWT on connect; refresh tokens supported; scope limited to user’s conversations.
* **SLOs:**
  + **Send→persist** (P95): **≤ 200 ms**;
  + **Send→deliver to online recipient** (P95): **≤ 2 s**;
  + **Email digest** for offline recipients: **≤ 15 min** batch.
* **Ordering:** per‑thread **monotonic sequence**; client de‑dupes by message.id.
* **Idempotency:** client sends client\_msg\_id (UUID); server returns same on echo. Retries safe.
* **Storage:** messages saved before fan‑out; **virus scan** runs async; any flagged attachment is hidden with a “Removed” notice.

## 17.4 Abuse, safety & rate limits (ties to §5 Risk)

### 17.4.1 Rate limits (default; Admin‑tunable 20.I)

* **New threads**: **5/day** per user (rolling 24h).
* **Messages**: **30/hour** per user (sliding window).
* **Attachments**: **15/day** per user; **5/day** per thread.
* **Link count**: warn when >2; optional block at >5/day.
* **Burst control**: if a user sends >5 messages in 30s → slow mode (1 msg / 10s) for 10 min.

### 17.4.2 Block, mute, report

* **Block**: prevents future messages **both ways**; shows “Blocked” label in header.
* **Mute**: stops notifications on a thread; keeps in inbox.
* **Report**: reasons (Harassment, Spam, Scam, Hate, Privacy, Other) + optional screenshot → creates **mod.case** (20.B) with SLA.

### 17.4.3 Spam heuristics (server‑side, MVP)

* URL density, repeated phrases, new account <24h + high velocity, profanity score, known bad IP/device.
* **Decisions**: Allow + monitor, **CAPTCHA challenge** (on next send), Queue Review, or Block. All decisions logged to risk.signal\_log (§5.13).

## 17.5 Privacy, security & compliance

* **Content sanitization:** strip HTML; escape special chars; anti‑XSS sanitizer on display.
* **Attachment hardening:** image type sniffing; EXIF strip; server‑side thumbnailing; **AV scan**; S3 **quarantine** bucket before release.
* **PII/PHI warnings:** inline warning in composer: “Don’t share sensitive info (SSN, medical records).”
* **Encryption at rest/in transit:** DB + object storage encrypted; TLS for all connections.
* **Access scopes:** Organizer shared inbox respects role scoping; staff viewing requires “view\_messages” scope + reason prompt; all staff views logged to admin.audit\_log.
* **Retention:** messages kept **24 months** unless legal hold (§6.7); DSAR deletes remove sender’s messages where permissible and anonymize counterpart name.

## 17.6 Data model (extends §8)

These build on §8 message.thread, message.participant, message.message.

**Additions / clarifications**

* message.thread
  + id (uuid), context enum('general','reward'), campaign\_id nullable, donation\_id nullable, subject text, opened\_by\_user\_id,
  + last\_msg\_at, last\_msg\_snippet, policy\_snapshot ('anyone'|'donors'|'off' at creation), archived\_for jsonb (user‑scoped), muted\_until jsonb (per user).
* message.participant
  + (thread\_id, user\_id) PK, role ('sender'|'recipient'|'staff\_proxy'), blocked bool, muted bool, unread\_count int, last\_read\_seq bigint.
* message.message
  + id uuid, thread\_id, sender\_id, seq bigint (auto‑increment per thread), body\_text, attachments jsonb[], flags jsonb (e.g., {tombstoned: true}), created\_at, deleted\_at nullable, client\_msg\_id.
* message.attachment (optional table if you prefer rows)
  + id, thread\_id, message\_id, file\_ref, mime, size\_bytes, width, height, alt\_text, scan\_status ('pending','clean','infected').
* **Indexes**:
  + thread (campaign\_id, context), message (thread\_id, seq), participant (user\_id, thread\_id), thread (last\_msg\_at DESC).

## 17.7 Organizer shared inbox (campaign & org)

* **View:** Team cards at top (Lead/Co‑Lead/Support). Tabs: All, Reward, Assigned to me, Muted, Archived.
* **Reply identity:** Replies are “from the campaign” with small “sent by {staff name}” line visible to staff only (donor sees campaign).
* **Assignments:** any staff can **assign** a thread to self; system auto‑assigns Reward threads to **Support** when status changes to **Pending**.
* **Outbound limits:** Only Lead/Co‑Lead can start **new** general threads **as the campaign**; Support is **reply‑only**.

## 17.8 Message lifecycle & actions

* **Send** → persist → fan‑out → local append.
* **Delete (sender only):** within **10 minutes** hard window; tombstone remains with timestamp. Staff can **Remove** messages (moderation action) → “Removed by moderation” tombstone.
* **Archive:** per user; moves thread to Archived; unarchive on new incoming message.
* **Mark unread:** sets unread\_count+1 and resets last\_read\_seq.
* **Pin** (Phase‑2): staff pin important reward threads.
* **Read receipts / typing indicators** (Phase‑2): disabled in MVP for privacy & simplicity.

## 17.9 Notifications & preferences (ties to §18)

* **Triggers:** new message (if recipient not active in thread), assignment changes, moderation removal.
* **Channels:** In‑app (always), Email (default ON), SMS (default OFF; per‑topic opt‑in).
* **Batching:** email digests **per thread** every **15 minutes** (if multiple messages arrive).
* **Quiet hours:** respected (18.4); security/finance overrides not used here.
* **Content:** email shows **sender name**, **campaign name**, and **short snippet** (first 120 chars, no links). CTA → “View message” (login required).
* **Preferences UI:** Portal → Notifications → “Direct messages” (In‑app required; Email toggle; SMS toggle).

## 17.10 Search & discovery (within inbox)

* **Inbox search:** subject/snippet/participant names; filter by context, campaign, date.
* **No global DM search** across users (privacy).
* **Org Admin** can search across **their org’s** campaigns (staff scope).

## 17.11 APIs (contract‑level)

REST or GraphQL; below are REST‑style for clarity.

* POST /api/dm/threads  
  **Body:** { target\_entity: {type:'user'|'campaign'|'org', id}, context:'general'|'reward', donation\_id?, subject?, body, attachments[] }  
  **Errors:** policy\_blocked, rate\_limited, anonymous\_not\_allowed, campaign\_dm\_off.
* GET /api/dm/threads?folder=inbox|archived&context=&campaign\_id=&q=…&page=…
* GET /api/dm/threads/:id → thread + messages (paginated by seq).
* POST /api/dm/threads/:id/messages → { body, attachments[], client\_msg\_id }.
* POST /api/dm/threads/:id/actions → { mute, unmute, archive, unarchive, mark\_unread }.
* POST /api/dm/threads/:id/block / report → { reason, details, screenshot\_ref? }.
* **Staff:** POST /api/admin/dm/threads/:id/remove\_message (moderation); requires scope + reason.
* **WebSocket:** /ws/messages → events: thread.created, message.created, message.deleted, thread.updated, assignment.updated.

**Idempotency:** client\_msg\_id dedupes message.created.

## 17.12 Analytics & instrumentation (ties to §20.T)

**Events (suggested):**

* dm\_thread\_start{context, entity\_type, entity\_id}
* dm\_message\_send{context, has\_attachment, link\_count}
* dm\_message\_receive{context}
* dm\_thread\_assign{assignee\_role}
* dm\_thread\_mute|archive|block|report{reason}
* reward\_dm\_from\_claim\_page{tier\_id}

**KPIs & dashboards:**

* DM volume/day; median response time (organizer side); report rate; block rate; spam hit‑rate; reward thread resolution time.

## 17.13 A11y & performance standards (inherits §4)

* **Keyboard**: full navigation & send; focus returns to thread list after archive; live region announces new messages.
* **Screen readers**: thread titles are h2; message items announce sender and timestamp; attachments have **alt text/captions**.
* **Performance**: paginated fetch (50 messages per page); virtualized list; image lazy loads; Web Vitals budgets respected.

## 17.14 Admin console integrations (ties to §20)

* **Trust & Safety → Messaging tab**: abuse queues, evidence, remove message, lock thread, suspend sender (platform‑wide).
* **Finance/Rewards**: from a donor/campaign record, “Open reward DM” deep‑link.
* **Support**: “Convert to ticket” (sends thread transcript to Helpdesk; stores ticket id on thread).
* **Config**: rate limit knobs; attachment types/size caps; profanity filters; DM default policy (global); org policy overrides.

## 17.15 Edge cases & rules

* **Campaign suspended** → New messages blocked; existing threads readable with banner: “Organizer currently unavailable.”
* **Donor DSAR deletion** → remove donor messages where allowed; **reward threads**: donor name becomes “Removed User”; organizer messages preserved.
* **Attachment infected** → hide with “Attachment removed”; notify sender; store scan result.
* **Entity switched DM policy to Off** → existing threads still reply‑able by organizer; new inbound blocked with friendly copy.
* **Blocked user tries to message** → show “You can’t message this recipient.”
* **Team member tries to view organizer inbox** → blocked (policy & permissions).

## 17.16 Microcopy (shipping)

* **Composer placeholder:** “Write a message…”
* **PII warning (inline help):** “For your safety, don’t share sensitive information (passwords, SSN, medical records).”
* **Policy (Donors‑only):** “Only donors can message this organizer.”
* **DM Off:** “This organizer isn’t receiving direct messages.”
* **Report confirm:** “Thanks—our team will review this conversation.”
* **Block confirm:** “Block **{name}**? They won’t be able to message you.”
* **Attachment limit:** “Up to 3 images (5 MB each).”
* **Infected file:** “Attachment removed for safety.”
* **Suspended organizer banner:** “Messaging is unavailable while this campaign is under review.”

## 17.17 Acceptance criteria (MVP)

1. **Policy gating** works (Anyone/Donors‑only/Off) on every entry point.
2. **Thread context** attaches (campaign/reward) and is visible to organizer staff per role matrix.
3. **Shared inbox**: Lead/Co‑Lead full access; Support reply‑only on reward threads; Members have no organizer inbox access.
4. **Privacy**: emails/phones hidden; anonymous donors cannot DM; “Hide name publicly” donors can.
5. **Delivery**: messages persist then fan‑out; WS/SSE fallback; SLOs met.
6. **Abuse controls**: rate limits, block, mute, report → moderation case; spam heuristics active; CAPTCHA challenge when flagged.
7. **Security**: sanitization; AV scan; EXIF strip; staff access audited.
8. **Notifications**: in‑app, email digest; preferences respected; quiet hours observed.
9. **A11y**: keyboardable, SR‑friendly, live region announcements.
10. **Retention & DSAR**: 24‑month retention; anonymization/deletion rules applied.
11. **Admin**: moderation removal works and displays tombstones; DM knobs adjustable; evidence export to helpdesk.

## 17.18 QA checklist (tie to §22)

* Start DM from entity profile with policy **Anyone**/**Donors‑only**/**Off** (expect correct gating).
* Reward claim → “Contact organizer” launches reward‑context thread; organizer Support can reply.
* Rate limits enforce (5 new threads/day; 30 msgs/hour) with friendly errors; CAPTCHA pathway tested.
* Block/mute/report flows; moderation removal; tombstones visible.
* Attachment flows: valid image, oversized file, infected file (simulate) → quarantine & removal message.
* WS/SSE fallback: live delivery tested; offline → email digest in ≤15 minutes.
* A11y: keyboard‑only, SR reads sender & time; focus order sane; new message announced.
* DSAR delete: donor anonymized in reward threads; organizer messages persist.
* Analytics: events fire with correct payloads; dashboard tiles populate.

## 17.19 Roadmap (Phase‑2/3)

* **Phase‑2:**
  + Read receipts & typing indicators (opt‑in); push notifications; SMS bridge (sender‑masked); link unfurl (server‑side, safe list); pinned threads; bulk actions.
* **Phase‑3:**
  + Group threads (multi‑participant) for org support teams; **email bridge** (reply by email); E2E encryption (scoped pilot, would limit moderation features); ML‑assisted abuse detection.

## Section 17B — Wireframe callouts

Use these as annotation layers on your Figma frames. Each callout includes content, behavior, a11y, and analytics tags.

### A) Inbox — Desktop (two‑pane)

1. **Global header**
   * Left: product logo → portal home.
   * Center: **Inbox** title.
   * Right: Notifications bell (unread dot), Profile menu.
   * **A11y:** <h1>Inbox</h1>; first focus here on route change.
2. **Search bar (threads)**
   * Placeholder: “Search by name or campaign”.
   * Debounced query; filters contextually.
   * **A11y:** role="search", aria-label="Search messages".
   * **Event:** dm\_search{q\_len}.
3. **Filter strip (chips)**
   * Chips: **All**, **Reward**, **Assigned**, **Archived**, **Muted**.
   * Pill shows counts; “Reward” pill uses accent color.
   * **Event:** dm\_filter\_click{filter}.
4. **Start new message (optional)**
   * Button “New message” (hidden if entity policy = Off for all).
   * Opens **Start DM** modal (select target user/org/team/campaign).
   * **Policy gate:** show donors‑only lock if user isn’t a donor.
   * **Event:** dm\_thread\_start\_open.
5. **Thread list (left rail)**
   * **Row contents:**
     + Avatar (entity) + status dot (muted/archived overlay icons).
     + **Title line:** “{Display Name or Campaign}” + context pill (**Reward**/**General**).
     + **Snippet line:** last sender name + 80‑char preview (links stripped).
     + **Meta:** timestamp (relative), unread badge (count).
   * **States:** loading skeleton (3–6 rows); empty state (“No messages yet”).
   * **Keyboard:** Up/Down selects, Enter opens.
   * **Event:** dm\_thread\_open{context}.
6. **Pagination / infinite scroll**
   * Append on scroll end; show spinner; preserve scroll position.
   * **Perf:** batch 25 rows.
7. **“Shared Inbox” banner (organizer only)**
   * Shows members with avatars (Lead/Co‑Lead/Support).
   * CTA: “Messaging settings” → policy/roles page.
8. **Unread counter**
   * Pill on each thread; global count on header bell.
   * **A11y:** aria-live="polite" for unread changes.

### B) Thread — Desktop (General context)

1. **Thread header**
   * Left: entity avatar + name (click opens **profile page**).
   * Subline: “General message” + campaign name (if started from campaign).
   * Right actions: **Mute**, **Archive**, **Report**, **Block** (3‑dot menu), **Assign** (organizer only).
   * **A11y:** <h2> thread title; buttons have text labels.
   * **Events:** dm\_thread\_mute|archive|block|report|assign.
2. **System banner (conditional)**
   * Examples: “This organizer isn’t receiving new messages”; “Thread archived”; “You’ve blocked {name}”.
   * Inline info style; dismissible where appropriate.
3. **Message list (virtualized)**
   * **Bubble** layout; alternating sides; timestamps (relative) under each bubble.
   * Sender name (organizer team replies show campaign as sender; staff‑only sublabel “sent by {Alice}”).
   * **Special states:**
     + Deleted/tombstoned: “Message deleted by sender”.
     + Removed by moderation: “Removed by moderation”.
   * **Attachments:** image thumb; click → lightbox viewer (Esc to close, arrow keys to navigate).
   * **A11y:** list has role="list", each message role="listitem", readable order top→bottom; new deliveries announced via polite live region.
   * **Perf:** batch 50; lazy load older via “Load more” above first message.
   * **Event:** dm\_message\_receive.
4. **Reward link chip (if thread is campaign‑general with recent donation)**
   * Subtle chip: “Reference a reward?” → opens picker of donor’s matching rewards (last 90d).
   * Selecting converts context to **reward** thread (or attaches reward anchor to next message).
   * **Event:** dm\_reward\_reference\_open|select.
5. **Composer**
   * Multiline field (max **2,000 chars**); soft counter; Shift+Enter newline.
   * Attachment button (up to **3** images, **5 MB** each).
   * Link limit hint: “Keep links to 2 per message.”
   * Inline safety hint: “Don’t share sensitive info (passwords, SSN, medical records).”
   * Disabled state: if blocked or thread locked.
   * **Buttons:** Send (primary), Attach (secondary).
   * **A11y:** label “Message text”; character count has aria-live="polite".
   * **Events:** dm\_message\_send{has\_attachment, link\_count}.
6. **Errors & guards (inline)**
   * Oversize/unsupported file → inline error below composer.
   * Too many messages → “You’re sending messages too quickly” + slow‑mode timer.
   * Profanity/harassment hit → soft warning with “Send anyway” (if allowed) or block by policy.
   * CAPTCHA step‑up (modal) for flagged senders.

### C) Thread — Desktop (Reward context)

1. **Reward context bar (top of thread)**
   * Left: **Tier name** chip (e.g., “Tier 2 • Signed Book”), amount, donation date/time.
   * Middle: donor’s **delivery type** (Physical/Digital) & claim status (Unclaimed/Claimed).
   * Right: **Open reward record** button → takes organizer to Rewards table row.
   * **A11y:** bar has summary text; assistive labels for the status.
2. **Organizer quick facts (right info panel—optional)**
   * Collapsible card with donor shipping address (if provided), claim note, tracking number (if any).
   * View‑only in DM; edits happen in Rewards table.
   * **Privacy:** only visible to Organizer/Support; donors do not see this panel.
3. **Status webhook chips (read‑only mirror)**
   * If fulfillment status changes while viewing, show toast: “Updated to Pending by {user}”.

### D) Start DM modal (New message / Entity profile button)

1. **Recipient selector**
   * Tabs: **User**, **Organizer**, **Campaign**, **Organization**; searchable typeahead for each.
   * Policy preview: a small lock/label if **Donors‑only** or **Off**.
   * **Events:** dm\_start\_selector\_open|select.
2. **Access gates**
   * **Donors‑only:** modal body explains requirement + “Make a donation” CTA.
   * **Off:** explain “This organizer isn’t receiving messages.”
   * **A11y:** focus returns to invoker on close.
3. **Pre‑filled subject (hidden, used internally)**
   * “General message to {entity}” or “Reward Tier {n} for {Campaign}”.

### E) Mobile layouts (iOS/Android web)

1. **Inbox tab** in bottom nav
   * Icon + unread badge.
   * Single‑pane list; tap → pushes Thread screen.
2. **Thread screen (mobile)**
   * Header with back chevron, entity name, 3‑dot menu (Mute, Report, Block).
   * Composer as **safe‑area anchored** sheet; attachments open from OS picker.
   * **Perf:** min render jank; keyboard avoids overlaying input.
3. **Reward context (mobile)**
   * Collapsible info pill under header; tap to expand details.
4. **Empty states**
   * Inbox empty: friendly illustration + “Find a campaign to support and send a message.” CTA to Search.
   * Thread empty (brand new): tip bubble “Be respectful and don’t share sensitive info.”

### F) Notifications preview (email)

1. **Email subject**: “New message from {DisplayName} about {Campaign}” (if reward: “…about your reward”).
   * Body snippet (max 120 chars), CTA “View message” (no content reply).
   * Footer link to **Notification Preferences**.

### G) Accessibility checklist (screen‑level)

* **Focus order:** Header → Filters → List → Thread header → Messages → Composer.
* **Skip links:** “Skip to thread” link for keyboard users.
* **Live regions:** Unread counts & new message appended messages announced once.
* **Contrast:** meet AA on chips & metadata.
* **Motion:** reduce anims when prefers-reduced-motion.

### H) Analytics tags (add to Figma notes)

* dm\_thread\_start\_open, dm\_thread\_open, dm\_message\_send, dm\_message\_receive, dm\_filter\_click, dm\_search, dm\_thread\_mute|archive|assign, dm\_report, dm\_block, dm\_reward\_reference\_select.

# Section 18 — Notifications & Messaging

## 18.0 Scope & goals

* **Scope:** event triggers, routing (email/SMS/voice/in‑app), preference & quiet‑hour logic, digests, deduping & rate‑limits, deliverability/health, template versioning, admin controls, compliance.
* **Goals:** reliable delivery, minimal noise, legally compliant consent/opt‑out, clear copy, easy to manage in Admin Console.

**Channels (MVP):**

1. **Email** (transactional + limited marketing)
2. **SMS** (transactional only) with **voice fallback** for critical events
3. **In‑app (portal) notifications** (always on)
4. **Push** (Phase‑2)

**Vendors (suggested):** Email via SendGrid/Mailgun; SMS/Voice via Twilio (A2P 10DLC US).  
**Identity:** SPF/DKIM/DMARC for email; A2P brand & campaign registration for SMS (US‑only).

## 18.1 Architecture (high-level)

* **Event bus → Notifier**: System events emit payloads (donation.created, payout.failed, kyc.status\_changed, message.received, etc.).
* **Routing engine** applies **preferences**, **quiet hours**, **rate limits**, **coalesce windows**, and **fallback** rules.
* **Template service** renders content (uses Admin 20.H Template Manager).
* **Delivery adapters** (Email/SMS/Voice/In‑app) send and log **DeliveryAttempts**; in‑app stores read/unread state.

**Idempotency:** all events have a notification\_key (e.g., donation:1234:receipt) to prevent duplicates across retries.

## 18.2 Timezone, locale & formatting

* All **timestamps localized** to the recipient’s portal timezone (Section 0.F.35).
* **Currency** in USD (with USD symbol), thousand separators, two decimals where appropriate.
* Locale: **English‑only MVP**, but all templates accept {locale} for future i18n.

## 18.3 Event catalog & routing matrix

**Legend:** E = Email, S = SMS, V = Voice fallback, A = In‑app.  
**Quiet hours (QH):** 9pm–8am local (user‑configurable). Security/legal **ignore** QH.

### A) Account & Security

| **Event** | **Trigger** | **Default Channels** | **QH** | **Notes** |
| --- | --- | --- | --- | --- |
| Login from new device | new session/device | E + A | Ignore | Security category (mandatory) |
| 2FA code | user requests OTP | S (primary) → V fallback | Ignore | Voice if SMS undelivered within 2 min |
| Email change confirmation | user initiates | E + A | Respect | Link expires; step‑up if needed |
| Password changed | success | E + A | Ignore | Security notification |
| Session timeout | idle logout | A | Respect | In‑app toast + next login banner |

### B) Verification (KYC/KYB)

| **Event** | **Trigger** | **Default Channels** | **QH** | **Notes** |
| --- | --- | --- | --- | --- |
| ID verified / failed | Stripe Identity status | E + A | Respect | Friendly tips on fail |
| SSN/EIN verified / failed | Connect status | E + A | Respect |  |
| Compliance Hold placed / released | admin action or auto | E + S + A | Ignore | S critical; Voice only if payout imminently blocked (optional) |

### C) Donations & Receipts

| **Event** | **Trigger** | **Default Channels** | **QH** | **Notes** |
| --- | --- | --- | --- | --- |
| Donation receipt | donation.success | E + A | Respect | Always transactional; includes AoN banner if applicable |
| Donation failed/3DS needed | failure or action required | E + S + A | Ignore | S link to resume payment |
| Refund issued / updated | refund.completed / partial | E + A | Respect | Updated receipt attached |
| AoN not funded → auto‑refund | deadline pass | E + A | Respect | Clear subject & body |

### D) Rewards

| **Event** | **Trigger** | **Default Channels** | **QH** | **Notes** |
| --- | --- | --- | --- | --- |
| Reward claim needed | donation ≥ tier but claim incomplete | E + A (reminder cadence) | Respect | Portal banner persists |
| Reward status → Pending/Processed | organizer updates | E + A (+ S optional) | Respect | If tracking present, include link |
| Organizer added note (shared) | note shared | E + A | Respect |  |

### E) Campaign lifecycle & Teams

| **Event** | **Trigger** | **Default Channels** | **QH** | **Notes** |
| --- | --- | --- | --- | --- |
| Campaign published | organizer action | E + A | Respect |  |
| New donation (organizer) | donation.success | E + A (batched) | Respect | Batch multiple into one email per hour |
| Tier sold out (first time) | first reach | E + A | Respect |  |
| Team invite sent / accepted / expired | actions/time | E + A (+ S optional) | Respect |  |
| Ownership transfer completed | success | E + A | Ignore | Security tier |

### F) Payouts & Finance

| **Event** | **Trigger** | **Default Channels** | **QH** | **Notes** |
| --- | --- | --- | --- | --- |
| Campaign ended → funds on hold | end event | E + A | Respect | Show ETA window |
| Eligible for payout | checks pass | E + A | Respect |  |
| Payout requested | organizer | E + A (+ S optional) | Respect |  |
| Payout processing | status change | A | Respect |  |
| **Payout paid** | settled | E + A | Respect | Statement link |
| **Payout failed/returned** | failure/return | E + **S** + A → **V fallback** | Ignore | Critical; Voice if SMS fails in 5 min |

### G) Refund requests & Disputes

| **Event** | **Trigger** | **Default Channels** | **QH** | **Notes** |
| --- | --- | --- | --- | --- |
| Donor refund request opened | donor → organizer | E + A | Respect | 48h SLA |
| Organizer decision needed reminder | 24h elapsed | E + S + A | Respect |  |
| Chargeback opened | processor | E + A | Ignore |  |
| Chargeback decision | outcome | E + A | Respect |  |

### H) Messaging (Direct Messages)

| **Event** | **Trigger** | **Default Channels** | **QH** | **Notes** |
| --- | --- | --- | --- | --- |
| New DM received | message.create | A + E (default) | Respect | User can mute thread; SMS off by default |
| DM reported | report.create | A (to staff) | n/a | Routes to Mod queue |

### I) Support tickets & Admin

| **Event** | **Trigger** | **Default Channels** | **QH** | **Notes** |
| --- | --- | --- | --- | --- |
| Ticket created / updated | helpdesk | E + A | Respect |  |
| Moderator decision | case closed | E + A | Respect | Template with guidance |

## 18.4 Preferences, topics & quiet hours

* **Topics:** Security (mandatory), Donations, Rewards, Payouts, Teams, Verification, Messaging, Support, Marketing (opt‑in), System (mandatory legal).
* Users control **Email/SMS toggles per topic** (Section 10.K.28). Some are mandatory (Security, System).
* **Quiet hours:** default 9pm–8am local; **ignored** for Security and critical Finance (payout failure/returned).
* **Digest emails** (organizers): **Optional, default OFF** (your decision). Weekly digest at local time with donations summary, tasks, and top referrers.

**AC**

* **AC‑PREF‑1:** Mandatory topics cannot be disabled; UI explains why.
* **AC‑PREF‑2:** Quiet hours applied per channel; in‑app is unaffected.
* **AC‑PREF‑3:** Unsubscribe for Marketing via one‑click header; transactional emails include manage‑preferences link.

## 18.5 SMS specifics & voice fallback

* **Compliance:** A2P 10DLC registration; honor **STOP/UNSTOP/HELP**; store consent timestamp & source.
* **Content:** transactional only (OTP, receipts short confirm, payout alerts, refund reminders).
* **Linking:** branded short domain; append ?n= notification id for tracking.
* **Length:** 160‑char segments; aim for ≤ 2 segments.
* **Voice fallback:** For **OTP** and **payout failed/returned** (critical), if SMS undelivered after **2–5 minutes** (configurable), trigger **TTS call** with concise script and link via SMS resend if possible.

**Voice scripts (examples):**

* OTP: “Your verification code is **{code}**. It expires in five minutes. Do not share this code.”
* Payout returned: “We couldn’t deliver your payout for **{campaign}**. Please update your bank details in your dashboard.”

**AC**

* **AC‑SMS‑1:** STOP immediately suppresses further SMS except HELP/STOP confirm.
* **AC‑SMS‑2:** Voice fallback only fires for whitelisted events; logs link to original SMS attempt.

## 18.6 In‑app notifications (portal)

* **Notification Center:** bell icon with unread counter; list grouped by **Today / Earlier this week / Older**.
* **Item anatomy:** icon (category), title, one‑line body, timestamp (relative), CTA link, kebab menu (Mark read, Mute thread for DMs).
* **Toasts:** success/error toasts for immediate actions (claim saved, payment retry).
* **Retention:** 90 days in‑app; archived thereafter (searchable for 12 months via “Show archived”).

**AC**

* **AC‑APP‑1:** Real‑time updates via websockets/long‑poll; fall back gracefully.
* **AC‑APP‑2:** Clicking an item marks it read and navigates to the deep link.

## 18.7 Rate limits, batching & deduping

* **Per‑recipient rate caps:** default **20 emails/day**, **15 SMS/day** (configurable; Security exempt).
* **Coalescing windows:**
  + Organizer **new donations** → batch into one email per **60 minutes** with count & sum.
  + DM new messages → batched per thread (email summary every **15 minutes** if multiple).
* **Idempotency**: identical notification\_key within **24h** not re‑sent.

**AC**

* **AC‑RATE‑1:** Caps and windows configurable in Admin 20.I; changes audited.

## 18.8 Deliverability & health

* **Dashboards (Admin 20.J):** send volume, delivery, open/click, bounce/complaint, SMS DLR, voice ASR, per template metrics.
* **Monitoring:** provider webhooks update **DeliveryAttempt**; alert on bounce spikes or DLR < threshold.
* **Reputation:** warmup IPs if using dedicated senders; DMARC record enforcement; rotating SMS sender pools per A2P rules.

**AC**

* **AC‑HEALTH‑1:** Bounce/complaints → add to **SuppressionList** with reason; show in user preferences with self‑service re‑enable flow (email only).

## 18.9 Template system & content

* **Template Manager (Admin 20.H):** versioning, test send, variables validation, partials (headers/footers), A/B variants.
* **Style:** clean, mobile‑first email; concise SMS; respectful tone.
* **Localization‑ready:** {locale} placeholder; default English.

**Common variables:** {user\_name} {campaign\_title} {amount} {goal} {deadline} {payout\_id} {receipt\_url} {manage\_prefs\_url} {support\_url} {org\_name} {team\_member\_name}.

**Key templates (sample subjects & SMS):**

* **Receipt (donor email):** “Thanks—your donation to {campaign\_title} is complete”  
  **Body key lines:** Amount, Tip, Fees covered, Net to campaign, AoN rule if any.
* **Reward claim reminder (email):** “Finish your reward claim for {campaign\_title}”  
  **SMS:** “Finish your reward claim: {short\_link}”
* **Payout returned (email):** “Action needed: your payout was returned”  
  **SMS:** “Payout returned for {campaign\_title}. Update bank: {short\_link}”  
  **Voice fallback:** Script above.
* **KYC incomplete (email):** “Verify your ID to publish your campaign”
* **DM new message (email):** “New message from {sender\_name}” (batched if needed)

## 18.10 Data model (conceptual)

* **NotificationEvent**: id, type, payload\_json, subject\_id, subject\_type, producer, created\_at
* **Notification**: id, user\_id, event\_id, topic, channels[], status {queued|sent|suppressed|failed}, notification\_key, quiet\_until
* **DeliveryAttempt**: id, notification\_id, channel, provider\_id, status, error\_code, sent\_at, delivered\_at, opened\_at, clicked\_at
* **UserPreference**: user\_id, topic, channel, enabled, quiet\_hours {start,end,tz}
* **DigestSubscription**: user\_id, freq {weekly}, next\_run\_at, last\_run\_at
* **SuppressionList**: user\_id or address, channel, reason (bounce, complaint, STOP), added\_at
* **Template**: key, version, channel, body\_html/text, variables[]
* **InAppNotification**: id, user\_id, title, body, category, link, read\_at, created\_at

## 18.11 Acceptance Criteria (summary)

* **Routing logic** honors preferences, quiet hours, and mandatory topics.
* **Critical events** (OTP, payout returned) use SMS with **voice fallback** on undelivered.
* **Coalescing** reduces noise (batched organizer donation summaries).
* **In‑app center** shows real‑time notifications with mark‑read and deep links.
* **Templates** are versioned and testable; variables validated; A/B supported.
* **Deliverability** tracked end‑to‑end; bounces/STOP update suppression lists.
* **Timezone localization** applied to all times in messages.
* **Idempotency** prevents duplicates; retries use exponential backoff.
* **Admin controls** exist for config, templates, health monitoring, and suppression.
* **Compliance:** A2P STOP/HELP honored; unsubscribe for marketing; transactional manage‑preferences link provided.

## 18.12 Microcopy (ready to ship)

* **Manage prefs footer (email):** “You’re receiving this because of your {topic} settings. Manage your preferences at {manage\_prefs\_url}.”
* **SMS HELP reply:** “{brand}: Msg&data rates may apply. Reply STOP to cancel. Help: {support\_url}.”
* **Refund confirmation:** “We’ve issued your {partial/full} refund of **${amount}** for **{campaign\_title}**. Your updated receipt is attached.”
* **Organizer batch donations:** “You received **{count}** new donations totaling **${sum}** in the last hour.”

## 18.13 Roadmap (Phase‑2)

* Mobile **push notifications**;
* **Follow campaign/organizer** subscriptions;
* **Localization** (ES first);
* **Multi‑brand sender profiles**;
* **On‑device passkeys** for 2FA reductions (security comms).

# Section 18B — Notifications & Templates

**Scope:** End‑to‑end notifications system for **Email, SMS, Voice fallback, and In‑app**. Covers OTP/auth, KYC/KYB, campaigns, donations, rewards, payouts, team, DM, moderation, support tickets, and admin messages.

**Depends on:** §0, §3 (roles), §4 (UX/A11y), §5 (Risk & Abuse), §6 (Privacy), §7 (APIs), §8 (Schema), §10 (Portal/Prefs), §11 (KYC), §12–16, §17 (DM), §20 (Admin), §21–22 (Ops/QA).

## 18.0 Principles

1. **Right channel, right urgency** — critical = fast & redundant; informational = digest.
2. **Privacy‑first** — no sensitive PII in messages; never disclose other users’ data; honor “hide name/anonymous”.
3. **Deliverability** — SPF/DKIM/DMARC, warm IPs, suppression lists unified.
4. **Idempotent & observable** — every send is traceable; no duplicates on webhook replays.
5. **Consistent copy** — one template library with versioning; legal links; friendly tone.

## 18.1 Channels & defaults

| **Channel** | **Use** | **Default** |
| --- | --- | --- |
| **In‑app** | All transactional & system; always on. | **ON** (cannot disable) |
| **Email** | Receipts, confirmations, digests, DM notifications, KYC/KYB, support. | **ON** for transactional; **opt‑in** for marketing |
| **SMS** | OTP, payout returned, urgent KYC blockers, high‑risk donation actions (rare), delivery nudges (optional). | **ON** for OTP; other **opt‑in per topic** |
| **Voice (TTS)** | **Fallback** when SMS **fails** for critical items (OTP, payout returned). | **ON** for OTP/payout returned fallback |
| **Push** | — | Phase‑2 |

**Quiet hours** apply to Email/SMS/Voice (see §18.4). In‑app always shows immediately.

## 18.2 Topic taxonomy (subscriptions)

**System topics** (non‑disableable):

* Security & Auth (OTP codes, password resets, device alerts)
* Legal & Policy (ToS/Privacy updates where required)

**Transactional topics** (user can choose channel):

* Donations & Receipts (donor)
* Campaign Activity (organizer)
* Reward Claims & Fulfillment (donor + organizer)
* Payouts & Finance (organizer)
* KYC/KYB & Compliance (organizer/org admin)
* Direct Messages (sender/recipient)
* Team (invites, joins, role changes)
* Moderation (case updates to organizer)
* Support Tickets (user ↔ helpdesk)

**Digest topics** (toggleable):

* Organizer Daily Donation Summary
* Weekly Campaign Performance (organizer/org admin)
* DM Email Digest (per thread batching)

**Marketing topics** (opt‑in only):

* Platform updates, tips, featured campaigns (off by default)

**AC‑TOPIC‑1:** Preferences UI (§10.K) shows topics & channel toggles with clear labels and examples.

## 18.3 Routing logic (who gets what)

**General rules**

* **Primary recipient**: the actor or owner.
* **Secondary recipients**: limited (e.g., Co‑Lead for team changes; org admins for org‑wide).
* **SMS** is used only for **OTP**, **payout returned**, **KYC blocker** (if opted in), and **time‑sensitive reward nudge** (if opted in).
* **Voice fallback** triggers only when **SMS undelivered** or **throttled** and topic is **critical**.

**Examples**

* Donation succeeded → **Donor**: Email receipt + In‑app; **Organizer**: In‑app + optional Email instant or Daily digest.
* Reward claim submitted → **Organizer**: In‑app + Email; **Donor**: In‑app confirmation.
* Payout returned → **Organizer**: SMS → (if no DLR success) **Voice fallback**, + Email + In‑app.
* KYC failed → **Organizer**: Email + In‑app; **SMS** if opted into “Compliance alerts”.
* DM new message → Recipient: In‑app + Email **digest** (15‑min batching); SMS is **OFF by default**.

## 18.4 Urgency levels, quiet hours, batching

**Urgency levels**

* **Critical** (OTP, payout returned, suspicious login): bypass quiet hours; SMS(+voice fallback).
* **Important** (donation receipt, refund, KYC pass/fail, reward status): respect quiet hours; Email immediate; SMS only if opted in.
* **Informational** (new donation to organizer, DM notifications, updates): respect quiet hours; **batch/digest**.

**Quiet hours**

* **Default:** 9pm–8am recipient **local time** (user‑configurable in Preferences).
* Critical overrides apply; others queue and send at 8am.

**Batching windows**

* **Organizer daily donation summary:** send 8am local.
* **DM email digest:** 15 minutes per thread.
* **Campaign update to donors:** coalesce edits within 10 minutes to avoid spam.

## 18.5 SMS → Voice fallback logic (critical only)

**Eligible events:** OTP, payout returned, account security (suspicious login), rare KYC blocker.

**Flow:**

1. Attempt SMS via Twilio Verify/Programmable SMS.
2. If no DLR **delivered** within **2 minutes** or **carrier error**, check **voice consent** (collected during phone verify).
3. Trigger **TTS call** with short script; retry **once** if unanswered; leave concise voicemail only if user allows voicemail (pref toggle).
4. Log outcome in notif.delivery\_attempt and thread timeline.

**Copy style (TTS):** short, verify name, no sensitive data beyond **one‑time code or “check portal”** link phrase.  
**Compliance:** respect **STOP/HELP**; if user issued STOP, do not call except OTP per Verify policy and explicit consent.

## 18.6 Template architecture & versioning

* **Keys**: area.topic.variant (e.g., donation.receipt.default, payout.returned.critical).
* **Formats**: Email (HTML + text), SMS (text ≤ 160 chars core, can be concatenated), Voice (SSML/TTS), In‑app (title + body + CTA).
* **Variables**: {first\_name}, {campaign\_title}, {amount}, {goal}, {deadline\_date\_local}, {reward\_tier\_name}, {payout\_id}, {support\_link}, {preferences\_link}, etc.
* **Styling**: Email uses lightweight, responsive template; dark‑mode aware; always include text‑only part.
* **Legal**: Footer includes **company info**, **preferences**, **privacy**, **ToS**, **help**.
* **Versioning**: Each template has version and effective\_at; sends store template\_key and version for audit.
* **Test send**: Admin can send any template to a sandbox user/email with sample vars.

**AC‑TPL‑1:** Changing a template **does not** re‑render historical sends; each send logs its rendered content hash for audit.

## 18.7 Template catalog (v1.0 — priority set)

Below are **ready‑to‑ship copy blocks** (you will localize later if needed). Adjust brand voice as desired.

### A) Security & Auth

**OTP (SMS)** — security.otp.sms

{code} is your verification code. It expires in 10 minutes. If you didn’t request this, ignore this message.  
**Voice (TTS)** — security.otp.voice  
“Your verification code is **{code}**. It expires in **ten minutes**. If you didn’t request this, you can ignore this call.”  
**New device login (Email)** — security.device.email  
Subject: **New sign‑in to your account**  
Body: We noticed a sign‑in from **{city\_state}** on **{device}** at **{time\_local}**. If this wasn’t you, secure your account.

### B) Donations & Receipts (Donor)

**Receipt (Email)** — donation.receipt.email

Subject: **Thank you for donating ${amount} to {campaign\_title}**  
Body: “You donated **${amount}**{tip\_line}{cover\_line}. {aon\_line} View your receipt and manage preferences {cta\_link}.  
Tip line (if T>0): “ and added a **${tip}** tip to support our platform”  
Cover line (if CF>0): “ and covered processing costs”  
AoN line (AoN only): “Charged now; automatically refunded if the goal isn’t met by **{deadline\_date\_local}**.”  
**Refund confirmation (Email)** — donation.refund.email  
Subject: **Your refund for {campaign\_title}**  
Body: “We’ve processed your refund of **${refund\_amount}**. It can take 5–10 business days to appear on your statement. View details {cta\_link}.”

### C) Organizer — Campaign Activity

**New donation (Email digest)** — organizer.donations.daily\_digest.email

Subject: **Yesterday’s donations for {campaign\_title}**  
Body: “{count} donations totaling **${sum}**. Top gift: **${top\_amount}**. See all donors and trends {cta\_link}.”  
**Campaign published (Email)** — campaign.published.email  
Subject: **Your campaign is live**  
Body: “**{campaign\_title}** is live. Share your link: {share\_url}. Invite your team {team\_link}.”

### D) Rewards

**Claim required (Email)** — reward.claim\_needed.email

Subject: **Tell us where to send your reward**  
Body: “Your donation qualifies for **{tier\_name}** on **{campaign\_title}**. Add your details {cta\_link}. You can opt out if you prefer.”  
**Organizer status change (Email + In‑app)** — reward.status\_change.email  
Subject: **Your reward is {status}**  
Body: “**{tier\_name}** for **{campaign\_title}** is now **{status}**. {tracking\_line} View details {cta\_link}.”

### E) Payouts & Finance (Organizer)

**Payout ready → requested → paid** — payout.state\_change.email

Subject: **Payout {status}: {campaign\_title}**  
Body: “Your payout for **{campaign\_title}** is **{status}** {status\_detail}. Statement {cta\_link}.”  
**Payout returned (SMS → Voice fallback + Email)** — payout.returned.critical

* SMS: “We couldn’t deliver your payout for **{campaign\_title}**. Update bank details: {short\_link}”
* Email: Subject: **Action needed: payout returned** — Body with instructions & support link.
* Voice: “We couldn’t deliver your payout for **{campaign\_title}**. Please sign in and update your bank details to try again.”

### F) KYC/KYB (Organizer/Org Admin)

**ID verified** — kyc.verified.email — “Your identity is verified. You can now publish campaigns.”  
**ID requires retry** — kyc.retry.email — tips (lighting, edges visible); link to retry.  
**EIN verified** — kyb.ein\_verified.email — nonprofit badge info.  
**Compliance hold** — kyc.hold.email — reason and next steps.

### G) Direct Messages (DM)

**New message (Email digest)** — dm.new.digest.email

Subject: **New messages from {sender}**  
Body: “{sender} sent {count} message(s) in **{thread\_title}**. Read and reply {cta\_link}.”  
**Thread assigned (Organizer)** — dm.assigned.email — “You’re assigned to **{thread\_title}**.”

### H) Team

**Invite** — team.invite.email

Subject: **You’ve been invited to join {campaign\_title}**  
Body: “{inviter} invited you to the team. Accept your invite {invite\_link}. Expires in 7 days.”  
**Role change** — team.role\_change.email — “You’re now **{role}** on **{campaign\_title}**.”

### I) Moderation

**Case opened (Organizer)** — mod.case\_open.email — “We’re reviewing **{campaign\_title}**. Donations are temporarily paused.”  
**Resolution** — mod.case\_resolved.email — “Review complete. Status: **{outcome}**.”

### J) Support tickets

**Ticket created** — support.ticket\_open.email — “We’ve received your request **#{id}**. We’ll reply soon.”  
**Ticket updated** — support.ticket\_update.email — “There’s an update on **#{id}**.”

(Full template text will live in Admin Template Manager; the above covers the critical day‑1 set.)

## 18.8 Time zone, dates & numbers

* Display times in **recipient’s timezone** (saved on profile or inferred from last login).
* Dates like “Oct 23, 2025” (month short).
* Currency **USD** with thousands separators; round to cents on receipts.

## 18.9 Deliverability & suppression

* **SendGrid primary**, **Mailgun failover** (Section 7).
* **SPF/DKIM/DMARC** set; **List‑Unsubscribe** headers on digest/marketing emails.
* **Bounce & complaints** → add to notif.suppression (email); **STOP** on SMS → add to SMS suppression; show in user Preferences with re‑enable flow.
* **No tracking pixels** in receipts; link tracking optional and privacy‑respecting.

**AC‑DELIV‑1:** Bounces/complaints STOP further mail/SMS immediately (except OTP HELP/STOP confirms).  
**AC‑DELIV‑2:** Failover engages when delivery rate dips below threshold; logged with alert (§21.5).

## 18.10 In‑app notifications (UX)

* **Bell icon** with unread count; **Notifications Center** shows grouped by date: Today, Yesterday, Earlier.
* Each item: icon, title, 1–2 lines, timestamp, CTA.
* Filters: All / Finance / Messages / Campaign / Rewards.
* **Mark all read**; per‑item “Mute this type”.
* **A11y:** list semantics; keyboard navigation; aria-live="polite" for new items.

## 18.11 Link handling & security

* Links point to **first‑party domain**; avoid external shorteners.
* **Signed action links** (email change, invites) include short‑lived tokens; one‑time use.
* No query params that reveal PII; pass business ids (campaign slug/id) safely.
* For SMS, use **short brand domain** (your domain) with HTTPS.

## 18.12 Idempotency & deduplication

* Each notification event has a **notif\_key** = hash(source\_system, event\_id, recipient\_id, template\_key, version).
* Store in notif.send\_log with unique constraint on notif\_key.
* Retries (provider webhooks or our queue) check idempotency before send.

**AC‑IDEM‑1:** No duplicate sends for the same event/recipient/template, even on webhook replays.

## 18.13 Throttling & guardrails

* **Per‑recipient per‑minute** cap (e.g., 5 emails/min; 5 SMS/hour).
* **Digest coalescing** windows as above.
* **Threaded** DM: emails coalesce by thread within 15 minutes.
* **Emergency override** available to Admin (20.H) for security incidents.

## 18.14 Monitoring & SLOs (tie to §21)

* **SLI‑N1 Email receipt** delivered in ≤ **5 min** (SLO ≥ **99%**).
* **SLI‑N2 SMS DLR** for OTP/payout returned in ≤ **2 min** (SLO ≥ **98%**).
* Dashboards: send volume, delivery %, bounce/complaint rates, SMS DLR, voice connect rate, suppression growth.
* Alerts: bounce spike >1%, SMS DLR <85% 30‑min window, webhook failure rate >2%.

## 18.15 Preferences UI (Portal, §10.K)

* **Matrix view**: rows = topics, columns = channels (In‑app fixed ON, Email, SMS).
* **Quiet hours** controls; **voice fallback** consent toggle; **voicemail allowed** toggle.
* **Preview** shows example copy for each topic.
* **Save** persists to notif.user\_preference and privacy.consent\_log.

**Defaults (MVP):**

* Email ON for transactional; OFF for marketing.
* SMS ON only for OTP; OFF for others (user can opt in).
* DM email digest ON.

## 18.16 Admin Template Manager (tie to §20.H)

* Template list with keys, version, last edited, channels.
* Editor with **variables validator** (must supply sample data).
* **Preview** renders HTML/text/SMS/Voice.
* **A/B variants** (Phase‑2).
* **Audit log** for edits; **test send** to sandbox.

## 18.17 Data model (extends §8)

notif.user\_preference

- id, user\_id, topic (enum), channel ('email','sms','voice','inapp'), enabled bool,

quiet\_hours\_jsonb {start:'21:00', end:'08:00', tz:'America/New\_York'},

voice\_consent bool, voicemail\_ok bool, updated\_at

notif.suppression

- id, user\_id nullable, channel ('email','sms'), target (email or phone),

reason ('bounce','complaint','stop','admin'), created\_at

notif.template

- key, version, channel, subject\_tpl, body\_tpl\_html, body\_tpl\_text, ssml\_tpl, variables\_json, effective\_at, status

notif.send\_log

- id, notif\_key (unique), user\_id, channel, template\_key, version, subject\_rendered\_hash, body\_rendered\_hash,

status ('queued','sent','delivered','failed','bounced','complained'),

provider\_msg\_id, provider, error\_code, created\_at, delivered\_at

notif.inapp

- id, user\_id, type, title, body, cta\_url, read bool, created\_at, read\_at

## 18.18 APIs

* POST /api/notifications/test-send (admin; with template\_key + sample vars)
* GET /api/notifications/inapp (list, paginate, filters)
* POST /api/notifications/inapp/:id/read
* GET /api/notifications/preferences / PUT to update matrix
* Provider webhooks (/webhooks/sendgrid, /webhooks/mailgun, /webhooks/twilio) handled per §7.16.

## 18.19 Acceptance Criteria (summary)

1. **Topic matrix** implemented; Preferences UI shows accurate toggles & defaults; quiet hours respected.
2. **Critical events** use SMS with **voice fallback** when undelivered in 2 minutes; logs show both attempts.
3. **Receipts & refunds** delivered via Email with accurate, localized content; in‑app shows immediately.
4. **DM notifications** batch by thread (15‑minute digest).
5. **Idempotency** prevents duplicates; retries safe.
6. **Suppression** honored for Email/SMS; STOP/HELP works; voice consent respected.
7. **Admin Template Manager** supports versioning, test sends, and variable validation; edits audited.
8. **Monitoring** dashboards & alerts live; SLOs tracked; failover to secondary ESP works.
9. **Privacy**: no other users’ PII in messages; anonymous donors never revealed; secure action links.
10. **A11y & UX**: In‑app notifications navigable via keyboard/screen readers.

## 18.20 QA checklist (tie to §22)

* OTP SMS & voice fallback (force DLR fail)
* Donation receipt (Email + In‑app), refund update, AoN refund copy
* Payout returned: SMS → Voice fallback → Email → In‑app
* KYC retry and pass; EIN verified; compliance hold notice
* Rewards: claim needed; status pending → processed (donor + organizer)
* DM digest batching (send multiple messages within 15 min)
* Quiet hours deferral for non‑critical; override for critical
* Preferences: toggle channels per topic; voice consent; STOP/UNSTOP
* Suppression: simulate bounce/complaint; ensure no further sends
* Admin: edit template, preview, test send; verify old sends retain old version
* Analytics: send\_log populated; delivery attempts visible; alerts configured

## 18.21 Microcopy library (quick refs)

* **Quiet hours disclosure:** “We won’t text or email during your quiet hours (9pm–8am) unless it’s urgent.”
* **Voice fallback consent:** “If a critical text can’t be delivered, we may call you with an automated message. You can turn this off anytime.”
* **Unsubscribe footer (email):** “You’re receiving this because of your account activity. Manage your [notification preferences].”
* **SMS HELP/STOP:** “Reply HELP for help, STOP to stop texts. Msg&data rates may apply.”

## 18.22 Roadmap (Phase‑2)

* Push notifications (web & mobile).
* Per‑campaign subscriber updates for donors (opt‑in follow).
* A/B testing for subject lines and CTA copy.
* Smart throttling (deduplicate cross‑topic sends within a short window).
* Multi‑language templates and locale routing.

# Section 20 — Admin Console

**20.0 Scope & dependencies**  
A unified, role‑gated console for Support, Moderation, Compliance/KYC, Finance Ops, Content/KB, Growth/SEO, and Super Admin.  
**Depends on:** Sections 0, 3, 11, 12, 14, 15, 18.  
**Note on refunds:** This spec **updates** our earlier default—**no auto‑approval**. Organizer/Org Admin must approve refunds; Finance Ops can override per policy.

## 20.A Console architecture & access

**A1. Shape** — **Single Admin Console** with role‑based navigation. ✅ (your choice)

**A2. Staff auth** — **SSO + mandatory 2FA**. ✅

**A3. Sessions & re‑auth**

* Idle **auto‑logout after 30 minutes**.
* **5:00 minute warning modal** with live countdown and “Stay signed in” button.
* Step‑up re‑auth (password or OTP) for **dangerous actions** (suspend user/campaign, cancel payout, mass emails, role override).  
  **AC‑A3‑1:** Modal appears at T‑5:00; dismissing resets the 30‑minute timer.  
  **AC‑A3‑2:** If timer reaches 0 → save draft state & logout; “Restore session” available after login.

**A4. Global search** — Users, Campaigns, Donations, Payouts, Refunds, Disputes, Reports, Invites, RoleBindings. ✅

* Filters: date ranges, status chips, role facets; saved searches.

**A5. Impersonation** — **Super Admin & Support Leads** only; read‑only for PII; copy disabled; large **“Impersonating {user}”** banner. ✅  
**AC‑A5‑1:** Enter/exit logged in **AuditLog** (actor, IP, target).  
**AC‑A5‑2:** Download/Export disabled while impersonating.

**A6. PII protections** — Mask SSN/EIN/bank; show statuses only; redact anonymous donors in exports. ✅

**A7. Environments** — Distinct **Staging** vs **Production** with persistent environment banner. ✅

## 20.B Trust & Safety / Moderation (massively expanded)

**B1. Queues**

* **Reports (Donor‑submitted)** by reason: Fraud, Prohibited Content, Hate/Harassment, Privacy/Impersonation, Spam/Scam, Unsafe Medical Claims, Other.
* **Auto‑Flags**: content keyword hits (medical claims, prohibited items), donation velocity abuses, same‑card‑multi‑account, high‑risk BINs, excessive refunds.
* **Escalations**: Appeals from organizers; repeat offenders; cross‑campaign patterns.
* **Saved Views**: “P1 active >4h”, “Fraud signals high”, “Medical claims + links”.

**B2. Priority & SLAs** (you asked me to choose)

* **P1:** Safety/Fraud — respond within **4 business hours**.
* **P2:** Content/policy — **1 business day**.
* **P3:** Low severity — **3 business days**.  
  **AC‑B2‑1:** Breach badges when SLA exceeded; auto‑notify Moderator Lead.

**B3. Case tools**

* Evidence bundle (links, screenshots, donor statements).
* Compare campaign revisions (story diff, media diffs).
* **Actions**: soft warning, require edits, remove media/sections, **Suspend/Unsuspend campaign**, **Suspend/Unsuspend user**, geo‑block (if added later), restrict features (e.g., disable new team invites).
* Message organizer with templates; request proof (receipts, invoices).
* “Shadow review” (donations temporarily paused but page visible with “under review” banner).

**B4. Outcomes & close codes** (I chose a robust set)

* **No Action**, **Warning Issued**, **Content Removed**, **Suspended**, **Closed – Evidence Insufficient**, **Closed – Confirmed Fraud**.
* Rationale mandatory; attach policy clause references.

**B5. Appeals**

* Organizer can appeal once per case; new evidence upload; different moderator reviews.  
  **AC‑B5‑1:** Appeals inherit P2 SLA; second decision final (unless Super Admin override).

**B6. Batch operations**

* Multi‑select campaigns → remove a flagged image across all; bulk message organizers; bulk suspend if confirmed ring.

**B7. Copy & UX**

* Donor‑side report receipt: “Thanks—we’ll review and update you if needed.”
* Organizer‑side notice: “Your campaign needs edits to continue accepting donations.”

## 20.C Compliance & KYC

**C13. KYC queue** — manual reviews for mismatches, EIN proof, name variance on bank vs ID. ✅

**C14. Document viewing** (I chose): **Stripe‑hosted viewer only**, no raw storage or downloads.  
**AC‑C14‑1:** Reviewer can see “Verified/Failed/Review” statuses; thumbnails show placeholders only.

**C15. Holds** (I chose a clear set)

* **Publish Hold** (blocks going live)
* **Compliance Hold** (blocks payout)
* **Reserve %** (case‑by‑case; 0–25% for 30–90 days)  
  **AC‑C15‑1:** Holds show on organizer Wallet with reason and target release date.

**C16. Outcomes** (I chose)

* **Verified**, **Verified with Notes**, **Unable to Verify**, **Request More Info** (auto email with checklist).  
  **AC‑C16‑1:** Outcome changes notify organizer with secure link.

## 20.D Finance Ops — Payouts, Returns, Negative Balance

**D17. Payout pipeline** (I chose stages)  
**Requested → In Review → Processing → Paid / Failed / Returned / Canceled**.

* Special badges: **Large payout (≥$50k)**, **Bank changed <24h**, **Compliance Hold**.

**D18. Actions** (I chose a wide set)

* Approve/Cancel, Trigger retry, Change ETA note, Add/Override reserve, Put/Release Compliance Hold, Edit statement memo, Recalculate statement, Download PDF/CSV, **Resubmit Returned**.  
  **AC‑D18‑1:** Dangerous actions require step‑up re‑auth.

**D19. Threshold approvals** (I chose dual‑approval scheme)

* **Dual approver** if **≥ $50,000** or **destination changed in last 24h**.
* Second approver must be a **different** Finance Ops or Super Admin.  
  **AC‑D19‑1:** Dual‑approval log shows both approvers and timestamps.

**D20. Returned payouts** (I chose **Yes**)

* When bank updated, Finance can **Resubmit now** without waiting.  
  **AC‑D20‑1:** New payout linked to the returned one for traceability.

**D21. Negative balance** (I chose robust aging)

* Buckets: **0–7d**, **8–30d**, **31–60d**, **60+ d**;
* Tools: contact log, repayment plan notes, partial offsets from future balances.  
  **AC‑D21‑1:** New payouts auto‑apply to negative balance first.

## 20.E Donations, Refunds & Disputes

**E22. Refund requests** — **To Organizer first**, visible to Finance; SLA reminders. ✅

**E23. Organizer refunds (policy change per your direction)**

* **No auto‑approval**. Every refund (full or partial) requires **Organizer or Org Admin approval** inside Admin/Organizer portal.
* **Finance Ops** can override or force refund (with reason & step‑up).
* Default SLA: **48 hours** for organizer action; then escalate to Finance Ops.  
  **AC‑E23‑1:** Refund cannot process until approver confirms via step‑up (OTP).  
  **AC‑E23‑2:** All refunds write to statement and donor gets an updated receipt.

**E24. Partial refunds** — **Yes**, with **reason code** (Duplicate, Donor Request, Reward Issue, Fraud, Other). ✅

**E25. Chargebacks/disputes** — Timeline + reminders; evidence kit (receipt, IP/device, reward status, communications). ✅  
**AC‑E25‑1:** Dispute outcomes logged; if loss, wallet adjusts; donor notified only if policy requires.

## 20.F Users & Campaigns Management

**F26. User admin view (tabs & actions)** ✅

* **Tabs:** Overview, Donations, Campaigns, Roles/Invites, Verifications, Flags, Tickets, Notes, Audit.
* **Actions:** Suspend/Unsuspend, Force‑assign role (with reason), Reset MFA, Send email, **Merge User** (new; see below), **Lock account** (temporary).
* **Merge User** tool (advanced): merge duplicates → move donations, rewards, roles; blocks if active payout or disputes; **Finance Ops** approval required.  
  **AC‑F26‑1:** Merge produces a summary diff and requires confirmation + reason.

**F27. Campaign admin view (tabs & actions)** ✅

* **Tabs:** Overview, Content (story/media/FAQ/updates), Team & Support, Rewards, Donations, Reports, Payouts, Flags, Notes, Audit.
* **Actions:** Edit content, Remove media, Suspend/Unsuspend, Require changes, Extend deadline (KWR only), Change goal upward (with audit), Close campaign early, **Feature on homepage**, **Pin to category**.  
  **AC‑F27‑1:** Feature/Pin shows effective date/time windows.

**F28. Bulk actions** ✅

* Content takedown across selected campaigns, targeted bulk emails (organizers/donors by filters) with rate limits, CSV exports with privacy rules.
* **CSV importer (admin only)** for curated lists (e.g., “Featured campaigns this week”).  
  **AC‑F28‑1:** Bulk actions have preview, estimated impact, and “type to confirm”.

## 20.G Support & Knowledge Base

**G29. Helpdesk integration** — Integrate with Zendesk/Intercom/Freshdesk; show inline ticket pane linked to user/campaign. ✅  
**G30. Macros & SLAs** — Default enabled; categorize by topic; escalations to Moderator/Finance as needed. ✅  
**G31. KB management** — Versioned articles, draft → review → publish workflow, scheduled publish, redirects, search synonyms. ✅  
**AC‑G31‑1:** KB edits require Editor + Approver; audit tracked.

## 20.H Notifications & Templates

**H32. Template manager** — Centralize email/SMS templates; variables with validation; preview/test send; versioning & rollback. ✅  
**H33. Localization** — Framework‑ready; **English‑only** MVP. ✅  
**Extras:** per‑template **A/B** variant support; visual editor; shared partials (headers/footers); dark mode preview.

## 20.I Configuration & Feature Flags

**I34. Config Center** — Admin‑editable settings:

* Tip options & default; “cover fees” mode; donation/payout caps; invite expiry; team seat caps; leaderboard default; AoN copy; report reasons; risk thresholds (velocity, same‑card); file size/quantity limits; nudge intervals; **default donation presets**; **max updates/day**; **commenting on/off** (when launched).
* **Announcement Banners**: site‑wide messages with start/end times (e.g., disaster relief notices).
* **Maintenance Mode**: disable donations globally (emergency), with public banner.  
  **AC‑I34‑1:** Changes require confirmation; high‑impact changes log to Audit.

**I35. Feature Flags** — Gradual rollouts, A/B tests, per‑segment targeting (staff, % of traffic). ✅

## 20.J Reports & Dashboards (expanded)

**J36. Dashboards** (expanded as you requested)

* **Executive**: Donations (gross/net), fees/tips, active campaigns, AoN vs KWR performance, payout pipeline, disputes trend, refund rate, KYC pass rate, share‑to‑donation conversion.
* **Trust & Safety**: reports volume by reason, SLA compliance, outcomes, repeat offenders, auto‑flag hit rate, false‑positive rate.
* **Finance**: payouts due/processing/returned, large payout approvals, negative balance aging, statement reconciliation health.
* **Product & Growth**: conversion funnels (visit→donation), tip opt‑in rate, cover‑fees rate, device mix, referral/member attribution performance, top channels/UTMs.
* **Rewards**: claim rates by tier, fulfillment status aging, on‑time % (14/30/45d).
* **Support**: ticket volume, SLA adherence, CSAT, top categories, macro usage.  
  **J37. Exports** — Scheduled CSVs; secure S3 links; PII rules applied. ✅  
  **J38. Custom report builder** (admin power users): dimensions/measures picker with privacy guards.  
  **AC‑J‑1:** Scheduled exports require recipients list, frequency, retention time, and purpose.

## 20.K Audit & Governance (expanded)

**K38. Audit Log** — Record actor, action, target, before/after snapshot, IP/device, step‑up method, timestamp; immutable; filterable; exportable. ✅

* **Advanced:** saved queries (e.g., “payout overrides last 30d”), anomaly highlights (burst of suspensions).  
  **K39. Retention** — Logs 24 months; tickets/KB 36 months; purge on legal request. ✅  
  **K40. Legal holds** — Freeze deletion for specific cases/users/campaigns. ✅  
  **K41. PIIR (PII Request) Desk** — Staff‑only triage for privacy requests (ties to 20.U DSAR).  
  **AC‑K‑1:** All deletions/holds recorded with case ID & approver.

## 20.L Accessibility & UX conventions (expanded)

**L41. Console accessibility** — Keyboard‑navigable queues, color‑blind‑safe chips, sticky headers, high‑contrast mode toggle, skip‑to‑content, ARIA for bulk selects and tables, reduced‑motion setting.  
**L42. Saved views/filters** — Yes, with shareable links. ✅  
**L43. Accessibility QA assistant** — Inline checker for content editors: headline levels, alt‑text missing, link text clarity; warns before publish.  
**AC‑L‑1:** Content publish blocked if **required alt‑text** missing for images.

## 20.M Safety rails & rate limits

**M43. Dangerous actions confirmation** — “Type to confirm” for suspend, delete, cancel payout, mass email, mass refund, ownership transfer. ✅  
**M44. Rate limits** — Export, mass email, refunds throttled (configurable). ✅  
**M45. Dry‑run mode** — Preview impact for bulk actions with sample result set.

## 20.N Microcopy & case messaging style

**Tone** — neutral, procedural, skimmable; include case ID in subjects. ✅  
**Templates** — “We need a quick edit”, “Your campaign is under review”, “Evidence request checklist”, “Payout returned—action needed”.

### ****NEW EXPANSION MODULES**** (to meet your “feature‑rich” requirement)

## 20.O Theme, Content & UI Controls (CMS)

* **Theme manager:** brand colors, logos, typography scale, button shapes, spacing presets; preview across key pages (Home, Campaign, Checkout).
* **Landing page builder:** reorder/enable modules (hero, featured rows, category carousels, testimonials, FAQ), edit copy & CTAs, upload media; schedule changes.
* **Campaign page layout controls:** toggle modules (updates/comments when launched), set default order (gallery → story → FAQ), set default donation presets.
* **Announcement banners:** dismissible site‑wide banners; segment by audience (guest, organizer, donor).
* **SEO basics:** title/meta defaults, robots rules, sitemap triggers; OG image template editor (brand overlay, progress bar token).
* **Copy library:** microcopy variables (“Donate”, “Support this campaign”), disclaimers, policy snippets; versioning & rollback.  
  **AC‑O‑1:** Publishing CMS changes logs diff & author; preview required before publish.

## 20.P Discovery, SEO & Curation

* **Manual curation:** feature campaigns on Home/category; “Editor’s Picks”.
* **Ranking controls:** trending algorithm weights (recent velocity vs total raised), tie‑breakers, freshness decay.
* **Search config:** synonyms, stopwords, typo tolerance, facets & boosts.
* **Redirects & canonicals:** manage slugs and 301s for renamed campaigns.  
  **AC‑P‑1:** Changing ranking weights shows **simulation** on sample query set.

## 20.Q Experiments & Growth

* **Experiment builder:** define variants (e.g., donation presets, tip default), target %, primary metric (donation conversion), guardrails (refund rate not ↑).
* **Ramps:** 1% → 10% → 50% → 100% with stop/rollback.
* **Post‑experiment report:** uplift, confidence, segment breakdowns.  
  **AC‑Q‑1:** Experiments can’t start without a primary metric and stop criteria.

## 20.R Integrations & Webhooks

* **Webhooks manager:** subscribe internal apps or verified partners to events (donation.created, payout.paid, refund.processed, reward.updated).
* **API keys:** rotate & scope; IP allowlists.
* **Stripe status panel:** webhooks health, last delivery, retry log.
* **Helpdesk & analytics integrations:** configure tokens; health checks.

## 20.S Ops & System Health

* **Job queues:** email sends, SMS, statement generation, webhook deliveries; retry counts; dead‑letter queue view.
* **Event health:** Stripe webhook success %, SMS delivery %, email bounce rate, authentication OTP success rate.
* **Incident panel:** set status page text; freeze risky flows (e.g., pause new campaigns) in emergencies.  
  **AC‑S‑1:** Health widgets show last 24h/7d graphs with thresholds & alerts.

## 20.T Reports & Dashboards (ext detail)

* **Drill‑downs:** click any card to pivot by category, campaign, geography, device.
* **Attribution:** donor acquisition source (UTM), team member codes; multi‑touch view (first/last touch).
* **Cohorts:** campaign cohorts by start month; donor cohorts by first donation date.  
  **AC‑T‑1:** All charts exportable (PNG/CSV); saved dashboards sharable.

## 20.U Data Privacy & DSAR

* **DSAR desk:** Verify identity; export data package; delete/anonymize where allowed; exclude on legal holds.
* **Email preferences:** manage subscriptions; re‑enable bounces with proof.
* **Suppression lists:** honor opt‑outs for mail/SMS.  
  **AC‑U‑1:** DSAR actions audited with requester identity proof note.

## 20.V Advanced Audit & Governance

* **Role edits journal:** every RoleBinding create/modify/revoke with actor and scope.
* **Policy versioning:** ToS/Privacy/Guidelines—store versions; map users to the version accepted.
* **Risk approvals ledger:** dual approvals for large payouts, user merges, mass actions.  
  **AC‑V‑1:** Ledger entries immutable; exportable for compliance.

## 20.W Acceptance Criteria (summary)

* **Auth & sessions:** SSO+2FA; idle logout 30m with 5m countdown; step‑up on dangerous actions.
* **Search & views:** global search + saved views.
* **Impersonation:** bannered, audited, read‑only PII, exports blocked.
* **Moderation:** queues, SLAs, batch actions, outcomes, appeals; organizer comms templated.
* **Compliance:** Stripe‑hosted doc views; holds (Publish, Compliance, Reserve%); outcomes notify.
* **Finance:** payout pipeline; dual approvals; returned resubmit; negative balance aging; statement edits logged.
* **Refunds:** **Organizer approval required**; Finance override; partial refunds with reason; SLA escalations.
* **Users/Campaigns:** merge tool with approvals; feature/pin; bulk ops with previews & type‑to‑confirm.
* **Support/KB:** integrated helpdesk; versioned KB with approvals.
* **Templates:** centralized, versioned, test sends.
* **Config/Flags:** tip/fees/caps/banners/maintenance; feature flags with ramps.
* **CMS/UI:** theme, landing builder, campaign layout controls, copy library, OG template editor.
* **Discovery/SEO:** curation, ranking weights, search synonyms, redirects.
* **Experiments:** builder with guardrails, ramps, reports.
* **Integrations/Webhooks:** events, API keys, IP allowlists, Stripe status.
* **Ops Health:** queues, delivery KPIs, incident controls.
* **Reports:** executive + functional dashboards, custom builder, scheduled exports.
* **Privacy/DSAR:** export/anonymize; suppression lists.
* **Audit/Governance:** full audit, role journals, policy versioning, approval ledger.
* **Accessibility:** WCAG 2.2 AA patterns; content checks.

## 20.X Microcopy (selected)

* **Idle warning modal:** “You’ll be signed out in **{mm:ss}** due to inactivity. Stay signed in?”
* **Dangerous action confirm:** “Type **SUSPEND** to confirm.”
* **Impersonation banner:** “You’re viewing the site as **{user}**. Some actions are restricted. [Exit]”
* **Refund approval request to Organizer:** “A donor requested a **{partial/full}** refund of **${amount}** for **{campaign}**. Approve or decline within **48 hours**.”
* **Returned payout:** “We couldn’t deliver your payout (reason: {code}). Update your bank to resubmit.”

## 20.Y Data model additions (conceptual)

* **AdminAction**(id, actor\_user\_id, action\_type, target\_type/id, before/after, ip, step\_up\_method, ts)
* **Case**(id, type=moderation|compliance|finance|support, priority, status, sla\_due, assignee, history[])
* **ModerationCase**(case\_id, report\_ids[], evidence[], outcome\_code, policy\_refs[])
* **ComplianceCase**(case\_id, hold\_type, reserve\_pct, outcome, notes)
* **PayoutCase**(case\_id, payout\_id, approvals[], events[])
* **RefundRequest**(id, donation\_id, requester\_id, status=pending|approved|declined, approver\_id, reason\_code, amount)
* **Experiment**(id, name, flags[], variants[], target, metrics[], status)
* **FeatureFlag**(id, key, on, rollout, segments)
* **Banner**(id, message, audience, start\_at, end\_at, dismissible)
* **CMSBlock**(id, page, position, content, version)
* **RiskApproval**(id, action, threshold, approver1, approver2, ts)
* **DSAR**(id, user\_id, request\_type, status, artifacts[], completed\_at)

**1) Purpose & Scope**

A no‑code / low‑code analytics builder inside the Admin Console that lets authorized staff create **ad‑hoc reports**, **pivot tables**, **visualizations**, and **scheduled exports** across Donations, Campaigns, Rewards, Payouts, Refunds, Disputes, KYC/Moderation, Team attribution, and Traffic (UTM) data—**with privacy guardrails** and performance limits.

**Primary use cases**

* Finance Ops: payout reconciliation, refunds/chargebacks monitoring, negative‑balance aging.
* Moderation/Compliance: report volumes, SLA adherence, outcome codes, repeat offenders.
* Product/Growth: conversion funnels, tip and cover‑fees uptake, UTM/channel performance, member referral attribution.
* Support: ticket SLAs, category trends.
* Exec: north‑star and KPI rollups by week/month.

**2) Roles & Permissions**

* **Who can build:** Super Admin; Finance Ops; Moderator Lead; Compliance Lead; Content/KB Editor (read‑only); **Report Builder** (permission flag assignable to any staff role).
* **Who can schedule/auto‑email:** Super Admin, Finance Ops, Report Builder.
* **PII rules:** Anonymous donors’ PII is **never** exposed; donor email/phone columns are **hidden** unless the user has **PII Export** permission (separate flag). Minimum‑aggregation thresholds apply (see §11).

**AC**

* Only roles with **Report Builder** see “New Report.”
* Attempting to add restricted fields without permission shows: *“You don’t have permission to include personally identifiable information.”*

**3) Data Sources & Semantic Layer (fields surfaced to Builder)**

**Core entities (read‑only analytics views)**

* DonationAnalytics (donation\_id, campaign\_id, donor\_id, amount\_gross, tip, fees, amount\_net\_to\_campaign, is\_anonymous, hide\_name\_publicly, funding\_model, created\_at, device\_type, state, utm\_source, utm\_medium, utm\_campaign, referral\_member\_id, chargeback\_flag, refund\_flag)
* CampaignAnalytics (campaign\_id, title, category, city, state, organizer\_user\_id, funding\_model, goal, start\_date, end\_date, status, team\_enabled)
* PayoutAnalytics (payout\_id, campaign\_id, amount, status, requested\_at, processed\_at, paid\_at, returned\_flag, hold\_reason, reserve\_pct)
* RefundAnalytics (refund\_id, donation\_id, campaign\_id, amount, reason\_code, approved\_by\_role, approved\_at)
* KYCAnalytics (user\_id, email\_verified, phone\_verified, id\_verified, ssn\_verified, ein\_verified, status, time\_to\_verify)
* ModerationAnalytics (case\_id, campaign\_id, reason, priority, status, sla\_due, breached\_flag, outcome\_code, time\_to\_close)
* RewardsAnalytics (campaign\_id, tier\_id, tier\_amount, claims, status\_counts: unfulfilled/pending/processed, avg\_days\_to\_pending, avg\_days\_to\_processed)
* TrafficAnalytics (session\_id, campaign\_id, visits, device, source/medium/campaign, landing\_page, member\_referral\_id)

**Dimensions** (examples): date (day/week/month), campaign, category, state, city, device, funding\_model, team\_member, utm\_source/medium/campaign, moderation\_reason, outcome\_code, payout\_status, refund\_reason, verification\_status.

**Measures** (examples):

* Counts: donations\_count, unique\_donors (distinct donor\_id), disputes\_count, reports\_count, reward\_claims\_count
* Sums: gross\_donations, tips, fees, net\_to\_campaign, refunds\_amount, payouts\_amount
* Ratios: conversion\_rate (donations/visits), tip\_uptake (% donations with tip), cover\_fees\_uptake (if tracked), chargeback\_rate, refund\_rate
* Time: time\_to\_payout\_days, time\_to\_verify\_hours, SLA\_breach\_rate
* Reward KPIs: tier\_claim\_rate, on\_time\_fulfillment\_rate (Processed within 30 days)

**AC**

* A data dictionary accessible in‑product lists each field (name, description, type, PII sensitivity, example value).

**4) UI & Interaction Model**

**Layout**

* **Left Sidebar:** Field picker (Dimensions, Measures), search, pinned favorites.
* **Center Canvas:** Drag‑and‑drop shelves: **Rows**, **Columns**, **Values**, **Filters**.
* **Top Bar:** Visualization selector (Table, Pivot, Line, Bar, Area, Pie\*, Map, Heatmap, Funnel, Cohort), time granularity, compare periods (YoY/DoD/WoW), Run/Refresh.
* **Right Panel:** Formatting (number formats, percent, compact K/M/B), conditional rules, legend, axis, color scale.
* **Footer:** Query status, row count, preview time, performance warnings.

\*Pie only enabled for ≤ 6 categories.

**Flows**

* **New Report → Choose base view** (Donations, Campaigns, Payouts, Refunds, Rewards, Moderation, Traffic).
* Add fields via drag‑and‑drop; apply filters; choose viz; Run.
* **Save** (name, description, visibility: private/shared), **Pin to Dashboard**, **Schedule**, **Export**.

**AC**

* Undo/redo history (last 20 actions).
* “Unsaved changes” guard on navigate away.

**5) Formula & Calculated Fields**

**Expression language** (Excel/SQL hybrid):

* Aggregates: SUM(), COUNT(), COUNT\_DISTINCT(), AVG(), MEDIAN(), PERCENTILE(value, 0.95)
* Logic: IF(cond, a, b), CASE WHEN, AND/OR/NOT, COALESCE()
* Date: DATE\_TRUNC('week', created\_at), DATEDIFF('day', start\_date, end\_date)
* Time series: ROLLING\_SUM(measure, 7), LAG(measure, 1), YOY\_GROWTH(curr, prev)
* Ratios: SAFE\_DIVIDE(a, b)

**Examples**

* **Net Margin %**: SAFE\_DIVIDE(SUM(amount\_net\_to\_campaign), SUM(amount\_gross))
* **On‑time Reward %**: SAFE\_DIVIDE(SUM(processed\_within\_30d), SUM(reward\_claims))

**AC**

* Calculated fields are validated with inline errors; PII‑unsafe formulas are blocked.

**6) Filters, Segments & Parameters**

* **Global filter bar** (date range, category, location, funding model, team member, UTM).
* **Parameter controls**: dropdowns or sliders that non‑builders can adjust on shared reports (e.g., “Top N states”).
* **Segment builder**: save common conditions (“US‑South campaigns”, “High‑risk donations”).

**AC**

* Filters can be locked (viewer cannot change) or adjustable.

**7) Visualizations & Options**

* **Tables / Pivot tables**: subtotals, grand totals, row/column groupings, top‑N filters.
* **Line/Bar/Area**: multiple series, dual axis (disabled by default to reduce misread), period compare overlays.
* **Map**: US state choropleth; hover tooltips; colorblind‑safe palette.
* **Heatmap**: e.g., donations by hour × weekday.
* **Funnel**: visits → checkout open → payment success → reward claim.
* **Cohort**: donor cohorts by first donation month with retention metric (return donations).

**AC**

* Each viz includes a “Describe this chart” info pop with data definition and caveats.

**8) Drill & Interactivity**

* **Drill‑down**: e.g., state → city → campaign.
* **Drill‑through**: open entity page (campaign/donation) in new tab (permissions‑aware).
* **Click to filter** within viz.
* **Annotate** points with notes visible to shared viewers.

**9) Sharing, Scheduling & Exports**

* **Share**: private (me), team (role‑gated), link with viewer parameters (no PII if not permitted).
* **Schedule**: email / Slack webhook daily/weekly/monthly at set time & timezone.
* **Exports**: CSV/XLSX (tables), PNG/PDF (charts), zipped CSVs for multi‑tab pivots.

**AC**

* Scheduled emails include “Report generated at {timestamp} (UTC)” and the applied filters.

**10) Performance & Limits**

* **Row cap**: default 100k rows per query (configurable).
* **Timeout**: 30s hard cap; long‑run jobs convert to **asynchronous snapshot** delivered to email.
* **Caching**: 5‑minute result cache keyed by query + filters; manual refresh button.
* **Heavy query warnings**: display estimated cost/time before run.

**11) Privacy & Compliance Guardrails**

* **k‑Anonymity**: if a group has < 5 donors, aggregation that could reveal identity is **redacted** or bucketed to “Other.”
* **PII mask**: email/phone hidden unless user has **PII Export**.
* **Anonymity**: anonymous donations are included in sums but **never** list-level.
* **Data retention**: respects platform retention windows.

**AC**

* Export tries with PII by non‑permitted user show a blocking modal with policy text.

**12) Accessibility**

* All charts and tables have alt descriptions; keyboard nav; colorblind‑safe defaults; WCAG 2.2 AA.

**13) Error States**

* **No data**: “No results for this range. Try widening your filters.”
* **Timeout**: “This query took too long. Try reducing fields or date range.”
* **Field conflict**: “Selected fields can’t be combined due to join ambiguity.” (Help opens data dictionary.)

**14) Data Model Additions**

* **Report**(id, name, owner\_id, visibility, base\_view, definition\_json, created\_at, updated\_at)
* **Dashboard**(id, name, owner\_id, layout\_json)
* **ReportSchedule**(id, report\_id, cron, channel, recipients[], timezone, last\_run\_at, active)
* **ReportRunLog**(id, report\_id, status, started\_at, finished\_at, row\_count, error)
* **FieldDictionary**(field\_id, name, type, table, pii\_level, description)

**15) Acceptance Criteria (Builder)**

* Drag‑and‑drop builder produces a valid query; persistence works.
* Privacy guardrails enforced on screen **and** in exports.
* Scheduled runs fire on time; failures notify owner with error log.
* Dashboard filters cascade to child reports (if linked).
* Row caps, timeouts, caching behave as specified.

**16) Starter Report Templates (bundled)**

1. **Donations by State (last 30 days)** — Map + table; dims: state; measures: gross\_donations, unique\_donors.
2. **Payouts Pipeline** — Table by status; measures: count, amount; filter: next 7 days.
3. **Rewards Fulfillment Aging** — Heatmap of days since campaign end vs status.
4. **Team Attribution Leaderboard** — Table by member; measures: amount, donations, conversion.
5. **Tip & Cover‑Fees Uptake** — Line over time with % tip and % cover fees.
6. **Trust & Safety SLA** — Bar chart of cases by priority with breach rate.
7. **Refunds & Disputes Trend** — Area chart of refunds and chargebacks over time.
8. **Conversion Funnel** — visits → checkout → success → reward claim.

**20.O.1 UI Mock Copy for CMS Controls (Theme + Landing + Campaign Layout + SEO + Banners + Copy Library)**

All strings are production‑ready. Tokens in **{curly\_braces}**.

**A) Theme Manager**

**Panel: Colors**

* Label: “Primary color”  
  Tooltip: “Used for buttons and key accents. For accessibility, ensure contrast ratio ≥ 4.5:1.”
* Label: “Secondary color”  
  Tooltip: “Highlights and secondary actions.”
* Label: “Background / Surface / Text”  
  Tooltip: “Set your global surfaces and base text color.”
* Validation error: “Contrast too low for normal text. Pick a darker color or increase contrast.”

**Panel: Typography**

* Label: “Font family”  
  Helper: “Use system fonts for best performance, or paste a hosted font URL.”
* Label: “Scale” (dropdown: Compact / Standard / Spacious)  
  Tooltip: “Controls vertical rhythm and readability.”

**Panel: Buttons**

* Label: “Corner radius” (slider)
* Label: “Hover style” (dropdown: Elevate / Underline / None)

**Actions**

* Button: “Preview changes”
* Button: “Save draft”
* Button: “Publish theme”
* Toast (success): “Theme published. Visitors will see the new style within a minute.”
* Toast (error): “Couldn’t publish theme. Try again or contact Support.”

**B) Landing Page Builder**

**Page header**

* Title: “Landing Page Builder”
* Helper: “Reorder sections, edit content, and schedule changes.”

**Section list (reorderable)**

* “Hero”
* “Featured campaigns”
* “Categories carousel”
* “How it works”
* “Testimonials”
* “FAQ”
* “Footer links”

**Section: Hero**

* Field: “Headline” — placeholder: “Fund hope. Fund change.”
* Field: “Subheadline” — placeholder: “Start a campaign or support one today.”
* Field: “Primary CTA label” — placeholder: “Start a campaign”
* Field: “Primary CTA link” — placeholder: “/start”
* Field: “Secondary CTA label” — placeholder: “Browse campaigns”
* Field: “Background image” — helper: “16:9, min 1600×900”
* Toggle: “Dark overlay on image”
* Preview note: “Use Preview to test contrast and mobile crop.”

**Section: Featured campaigns**

* Toggle: “Use manual curation”  
  Helper: “Pick exact campaigns to feature. Turn off to use trending.”
* Field: “Section title” — placeholder: “Featured right now”

**Section: Categories carousel**

* Field: “Section title” — placeholder: “Explore categories”
* Field: “Categories to show” — helper: “Leave blank to show all.”

**Global controls**

* Button: “Preview” (opens preview mode with a querystring, e.g., ?preview=draft)
* Button: “Schedule publish”  
  Modal fields: Start date/time, End date/time (optional), Timezone  
  Confirm copy: “Scheduled. We’ll publish on {date\_time}.”

**Warnings**

* On leaving with unsaved changes: “You have unsaved changes. Discard or save as draft?”
* On deleting a section: “Remove ‘{section\_name}’ from this page? This can be restored from version history.”

**C) Campaign Page Layout Controls**

**Panel: Modules**

* Toggle: “Show team leaderboard”
* Toggle: “Show recent donors & messages”
* Toggle: “Show updates feed”
* Toggle (future): “Enable comments (donors‑only)”

**Panel: Order**

* Drag the order of: Gallery • Story • FAQ • Updates • Team leaderboard.

**Panel: Donation widget defaults**

* Field: “Preset amounts” — helper: “Comma‑separated whole dollars. Example: 25,50,100,250”
* Toggle: “Show ‘cover fees’ option”
* Toggle: “Tip suggested”
* Dropdown: “Tip default” — values: 10% / 15% / 20% / None
* Tooltip: “Donors can always change this during checkout.”

**Actions**

* Button: “Save layout”
* Toast: “Campaign layout updated.”

**D) Announcement Banners**

* Field: “Banner message” — placeholder: “We’re supporting wildfire relief efforts. Learn how you can help.”
* Toggle: “Dismissible”
* Field: “Audience” — options: Everyone / Organizers / Donors / Guests
* Schedule: Start / End / Timezone
* Button: “Activate banner”
* Toast: “Banner activated.”
* Warning on overlap: “You already have an active banner. Continue and replace it?”

**E) SEO & Social**

**Global SEO**

* Field: “Default page title suffix” — placeholder: “| {brand\_name}”
* Field: “Default meta description” — helper: “Up to 160 characters; shown in search results.”
* Toggle: “Generate XML sitemap daily”
* Field: “Robots.txt rules” (multiline)

**OG Image Template Editor**

* Field: “Overlay title font size”
* Field: “Brand logo position” — options: Top‑left / Top‑right
* Toggle: “Show progress bar”  
  Tooltip: “Uses current raised/goal at image generation time.”
* Button: “Preview OG image”
* Toast: “OG template saved.”

**Campaign SEO override (per campaign via admin)**

* Field: “SEO title” — placeholder: “{campaign\_title} – Help {beneficiary}”
* Field: “Meta description” — placeholder: “{short\_description}”
* Field: “Canonical URL” — placeholder: “https://{domain}/{slug}”
* Field: “Slug” — helper: “Changing slugs creates a redirect.”

**F) Copy Library (Global Text System)**

**List view columns**: Key • Context • Current value • Last edited • Actions (Edit, History, Restore)

**Common keys & defaults**

* cta.start\_campaign: “Start a campaign”
* cta.donate\_now: “Donate now”
* label.goal: “Goal”
* label.raised: “Raised”
* label.days\_left: “Days left”
* disclaimer.rewards: “Rewards are provided by the organizer; not guaranteed by the platform.”
* tooltip.cover\_fees: “Helps the campaign receive your full intended amount.”
* notice.aon: “Charged now; automatically refunded if the goal isn’t met by {deadline}.”
* error.required: “This field is required.”
* empty.no\_results: “No results found. Try adjusting your filters.”

**Edit modal**

* Label: “New value”
* Helper: “Use tokens like {deadline}, {amount}, {campaign\_title} where supported.”
* Button: “Save” / “Cancel”
* Toast: “Copy updated.”
* “View history” shows prior values, editor, timestamp; Button: “Restore this version.”

**G) Dangerous Action Copy (CMS)**

* Delete section: “Type **DELETE** to confirm removing this section.”
* Publish theme: “Publishing will immediately update the site’s look and feel for all visitors.”
* Maintenance mode: “Donations will be temporarily disabled for all campaigns. Proceed?”

**H) Empty States**

* Theme Manager: “No theme changes yet. Start by picking a primary color.”
* Landing Builder: “Drag a section from the list to begin.”
* Copy Library: “No custom copy yet. Click any key to edit.”

**I) Save / Publish / Rollback**

* Save draft (toast): “Draft saved.”
* Publish (modal): “Publish these changes now?”
* Schedule (toast): “Scheduled for {date\_time}.”
* Rollback (modal): “Revert to **{timestamp}**? Current changes will be saved as a draft.”
* Rollback (success): “Rolled back to the selected version.”

**CMS Acceptance Criteria**

* All changes previewable before publish.
* Version history with diffs for Theme, Landing, Copy Library, OG template.
* Scheduling respects timezone and doesn’t overwrite newer drafts.
* Maintenance Mode banner shows to all users with configured message.
* Accessibility checker warns on missing alt text, low contrast in hero overlays, and too‑long meta descriptions.

# Section 21 — Engineering Runbooks, SRE & SLOs

## 21.0 Scope & goals

**Scope:** Production operations for the donations platform—checkout, webhooks, payouts, KYC/KYB, notifications, search/discovery, admin console, CMS, messaging.  
**Goals:** 1) Keep donating and payouts reliable; 2) Make incidents short and transparent; 3) Protect data & money; 4) Provide clear, repeatable playbooks.

**Assumptions:** Cloud infra; PostgreSQL 15+; object storage (S3‑class); CDN; observability stack (metrics, logs, traces, error monitoring).

## 21.1 SLIs & SLOs (with error budgets)

**Periods:** Monthly (28–31 days). **Blameless** postmortems when SLOs are breached.

### A) Checkout & Donations

* **SLI‑C1 Payment success rate** = succeeded PIs / (succeeded + failed + canceled PIs) (excl. user cancels during 3DS).  
  **SLO:** ≥ **99.90%** monthly. **Error budget:** 0.10%.
* **SLI‑C2 Checkout latency (P95)** from “Donate” click → PI outcome (success/fail).  
  **SLO:** ≤ **4.0s** P95.
* **SLI‑C3 Minimums guardrail accuracy** = % donations blocked < $5 that would have been accepted.  
  **SLO:** ≥ **99.99%** (i.e., false blocks ≤ 0.01%).

### B) Webhooks & Backends

* **SLI‑W1 Webhook processing time (P99)** from provider delivery → domain write.  
  **SLO:** ≤ **60s** for **99%** of events.
* **SLI‑W2 Idempotency correctness** = duplicate webhook events that resulted in duplicate domain writes.  
  **SLO:** **0** per month (strict).

### C) Payouts & Wallet

* **SLI‑P1 Payout status freshness**: banner/console updates within 2 minutes of provider event (paid/failed/returned).  
  **SLO:** **≤ 2 min** for **99%**.
* **SLI‑P2 Statement accuracy**: reconciliation diffs between Stripe and ledger.  
  **SLO:** **0.01%** of total monthly volume tolerance.

### D) KYC/KYB & Verification

* **SLI‑K1 Auto‑KYC pass latency (P95)**: Stripe Identity verified → portal status green.  
  **SLO:** ≤ **90s**.
* **SLI‑K2 Manual review SLA**: P2 cases closed within **1 business day**.  
  **SLO:** **≥ 95%**.

### E) Notifications

* **SLI‑N1 Receipt delivery (Email)**: delivered within **5 minutes** of donation.  
  **SLO:** **≥ 99%**.
* **SLI‑N2 SMS DLR (critical)** for OTP/payout returned within **2 minutes**.  
  **SLO:** **≥ 98%**.

### F) Discovery & Public Pages

* **SLI‑D1 LCP on Home/Category/Campaign (mid‑range mobile)**.  
  **SLO:** **≤ 2.5s** P75.
* **SLI‑D2 Search index freshness** (donation velocity reflected in Trending).  
  **SLO:** **≤ 15 min** for **95%**.

### Error budget policy

* If a product area burns >50% of its monthly budget mid‑period → **freeze non‑urgent releases** in that area, prioritize remediation.
* If 100% burned → **release block** (except hotfixes), **postmortem**, and **experiment pause** for that area.

## 21.2 Incident severities & comms

**Severity definitions**

* **P0 (Critical):** Checkout unavailable; widespread payment failures; data corruption; security breach; Payouts fail globally.
* **P1 (High):** Partial region/provider outage; prolonged webhook backlog; KYC flow broken; returns surge; SMS/OTP down.
* **P2 (Medium):** Single module degraded (e.g., updates feed), Admin issues, delayed emails.
* **P3 (Low):** Cosmetic/typo; non‑blocking bugs.

**Targets**

* **P0**: Acknowledge **≤ 5 min**, Mitigate **≤ 30 min**, Resolve **≤ 4 h**.
* **P1**: Ack **≤ 15 min**, Mitigate **≤ 60 min**, Resolve **≤ 24 h**.
* **P2**: Ack **≤ 1 h**, Resolve **≤ 3 d**.
* **P3**: Planned.

**Communication**

* Private: Incident Slack/MS Teams channel #inc-{YYYYMMDD}-{short}.
* Public: **Status page** updates (initiation, hourly, resolution).
* Users (email/SMS): only for user‑impacting P0/P1 as defined; clear next steps.

**Status page microcopy (templates)**

* **Identified:** “We’re investigating an issue causing {impact}. Donations may be affected. Next update in 30 minutes.”
* **Mitigating:** “A fix is being deployed. We’re monitoring recovery.”
* **Resolved:** “Incident resolved. Root cause and actions will follow in a postmortem.”

## 21.3 On‑call & escalation

**Rotation**

* **Primary SRE**, **Secondary SRE**, **Feature‑Owner Dev** (area on‑call), **Incident Commander (IC)** rotation weekly.
* Hours: **24×7** for Primary/Secondary; Feature‑Owner during business hours with backup.

**Escalation ladder**

1. Pager alerts → **Primary**.
2. If unacked in 5 min → **Secondary** + **IC**.
3. IC assembles responders (DBA, Payments SME, Notifications SME).
4. IC runs comms & updates status page.

**Paging policy**

* Quiet hours exceptions for critical alerts already applied (Section 18).

**Training**

* New on‑call completes **shadow week**, reads this section, performs **mock incident**.

## 21.4 Observability stack

* **Metrics**: service metrics (HTTP rates/latencies), business metrics (donation success, payout stages), queue backlogs, DB health.
* **Logs**: structured JSON; correlation IDs propagate (request\_id, donation\_id, payout\_id).
* **Tracing**: distributed tracing around checkout, webhooks, payout pipeline.
* **Errors**: real‑time error tracker (e.g., Sentry) with release/version tags.
* **Dashboards**:
  + **Checkout** (PIs, 3DS, declines, success rate),
  + **Webhooks** (ingest rate, error rate, age P95),
  + **Payouts** (pipeline counts by status),
  + **KYC** (pass/fail, manual review queue aging),
  + **Notifications** (email/sms send, DLR/bounce),
  + **DB** (replication lag, locks, slow queries),
  + **Jobs** (queue depth, retries, DLQ).

**AC‑OBS‑1:** Every alertable SLI has a chart; all dashboards link from a “Runbooks” index.

## 21.5 Alert rules (initial thresholds)

**Checkout**

* **P0:** Payment success rate < **98%** for 5 min; or payment error rate spikes 10× baseline.
* **P1:** Checkout latency P95 > **6s** for 10 min; 3DS challenge failure spike > 2×.

**Webhooks**

* **P1:** Event backlog age P99 > **5 min** for 10 min.
* **P0:** Stripe signature verification failures > **50/min** for 5 min (possible replay attack).

**Payouts**

* **P1:** payout.failed|returned rate > **2%** hourly or absolute count ≥ **10** in 30 min.
* **P0:** Finance queue can’t write to DB (deadlocks/locks) for 2 min.

**KYC**

* **P1:** identity.verification\_session.\* failures > **10/min** for 5 min.
* **P2:** Manual review queue > **100** for > 4 h.

**Notifications**

* **P1:** SMS DLR < **85%** over 30 min; OTP verify failures > **20%** over 15 min.
* **P2:** Email bounce > **2%** day‑over‑day.

**DB**

* **P0:** Primary unavailable; replication lag > **60s** for 5 min; connection saturation > **90%**.
* **P1:** Long‑running queries > **60s** count ≥ 10.

**Jobs**

* **P1:** DLQ non‑empty > **10 min**; queue depth > **50k** for 15 min.

**Search**

* **P2:** Index freshness > **30 min** for 15 min.

**Admin**

* **P2:** Feature flag service unavailable; CMS publish failures > 5 in 10 min.

**AC‑ALERT‑1:** Each alert links to the related **runbook** and dashboard.

## 21.6 Runbooks (step‑by‑step)

Each runbook has **What you see**, **Likely causes**, **Mitigation now**, **Validation**, **Follow‑ups**. All changes recorded in **admin.audit\_log**.

### R1 — Stripe Payments outage / degraded

**Symptoms:** Payment success rate drops; provider status red.  
**Mitigation now**

1. IC declares **P0**, update status page.
2. Toggle **Maintenance Mode: donations off** (Admin 20.I) **only if** majority failing; otherwise keep on and show banner “Intermittent payment issues.”
3. If Apple/Google Pay specific → temporarily **disable** those methods in config (20.I).
4. Increase **checkout retries** (14.H.31) to 1 immediate + 1 after 30s if safe.
5. Monitor provider status; capture correlation IDs.  
   **Validation:** Success rate returns ≥ 99.5%; error logs fall to baseline.  
   **Follow‑ups:** Postmortem; review retry strategy; add test to simulate PI failures.

### R2 — Webhook backlog growing (Stripe/Twilio/Email)

**Symptoms:** Age P99 > 5 min; DLQ growing.  
**Likely:** Provider delivery spike; consumer stuck; DB lock; poison message.  
**Mitigation now**

1. Scale consumers horizontally; ensure one‑stream‑per‑aggregate sequencing holds.
2. Identify **poison event** (repeating failure). Quarantine to **DLQ**; file bug.
3. If DB lock: find blocking query; kill safely; capture EXPLAIN.
4. For Twilio STOP storms: ensure suppression updates succeed (Section 18).  
   **Validation:** Age P99 < 60s; DLQ empty.  
   **Follow‑ups:** Add circuit breakers; improve dedupe; index tuning.

### R3 — Payouts failing/returned spike

**Symptoms:** payout.failed|returned > thresholds; organizer complaints.  
**Mitigation now**

1. IC **P1**; notify Finance Ops.
2. Check **Connect** status; if bank verification mismatches → place **Compliance Hold** with clear banner (11.5).
3. Trigger **Resubmit** workflow for returned payouts after organizer updates bank (20.D.20).
4. For widespread bank routing issues, send template notice to affected organizers (20.H).  
   **Validation:** New payouts succeed; failed/returned normalize.  
   **Follow‑ups:** Dual‑approval review; risk heuristics for bank changes <24h.

### R4 — KYC Identity failures surge

**Symptoms:** Identity fails > 10/min; organizers blocked from publish.  
**Mitigation now**

1. IC **P1**; status page note.
2. Check Stripe Identity status; if degraded, **relax step‑up** temporarily (disable selfie unless high‑risk).
3. Open **Compliance Review** queue for those blocked > 2 attempts; staff assist.  
   **Validation:** Pass rates recover; publish gate unblocks.  
   **Follow‑ups:** Improve retry tips; edge‑case sample set for vendor.

### R5 — SMS OTP/Delivery outage

**Symptoms:** OTP failure > 20%; DLR < 85%.  
**Mitigation now**

1. IC **P1**; toggle **Voice fallback** immediately (18.5).
2. If a specific carrier: route via alternate sender pool (A2P).
3. Temporarily allow **email OTP** for phone change flows.  
   **Validation:** OTP success ≥ 95% resumes.  
   **Follow‑ups:** Carrier escalation; sender reputation review.

### R6 — Email bounce spike / suppression explosion

**Symptoms:** Bounce > 2% day‑over‑day; sudden domain blocklisting.  
**Mitigation now**

1. Switch to **failover ESP** (Mailgun).
2. Pause non‑critical sends; keep receipts/payouts.
3. Run **list hygiene**; remove obvious traps; check DMARC/SPF/DKIM.  
   **Validation:** Bounce < 0.5%; delivery stabilizes.  
   **Follow‑ups:** Warmup plan; template tweaks; domain reputation audit.

### R7 — Database primary degraded / failover

**Symptoms:** Connection saturation; replication lag; read queries time out.  
**Mitigation now**

1. IC **P0**.
2. Put site in **Read‑only degraded mode** (donations off; browsing on) if needed.
3. Failover to replica (managed service or manual promote).
4. Check write‑ahead logs (PITR); ensure replicas align.  
   **Validation:** Latency normalized; errors gone.  
   **Follow‑ups:** Root cause (bad query, migration, spike); add rate limits/caches.

### R8 — Search index stale

**Symptoms:** Trending not reflecting donations; freshness > 30 min.  
**Mitigation now**

1. Re‑run **indexer** job; replay **Outbox** since timestamp.
2. If job is stuck on specific records, quarantine and continue.  
   **Validation:** Freshness < 15 min.  
   **Follow‑ups:** Improve idempotent upserts; add dead‑letter metrics.

### R9 — Fraud ring / spam DMs

**Symptoms:** Many new accounts, similar cards/IPs, DM abuse reports.  
**Mitigation now**

1. Increase **velocity & card‑BIN risk thresholds** (20.I).
2. Turn on **manual review for high‑risk** donation patterns (shadow block).
3. DM: enforce **Donors‑only** default for organizer DMs temporarily; rate‑limit new threads (10.S).
4. T&S to ban and **retro‑refund** if policy allows; audit all actions.  
   **Validation:** Abuse reports drop; chargeback exposure contained.  
   **Follow‑ups:** Add device fingerprinting/behavioral signals.

### R10 — CMS publish breaks layout / SEO regression

**Symptoms:** 500s on Home; LCP > 4s; wrong meta/canonicals.  
**Mitigation now**

1. Rollback to previous CMS version (20.O rollback).
2. Fix asset/alt text; re‑publish.  
   **Validation:** Lighthouse back ≥ 90.  
   **Follow‑ups:** Tighten pre‑publish checks; add visual diff tests.

## 21.7 Backups, restore & DR

**Backups**

* **Postgres**: daily full + **PITR** WAL every 5 min; **encrypted**, immutable bucket; **retention 30 days**.
* **Object storage**: versioning ON; lifecycle to IA/Glacier.
* **Configs/Flags/Templates**: nightly snapshot + on‑change export.

**DR objectives**

* **RTO** (time to restore): **60 min** for DB; **15 min** for stateless services.
* **RPO** (data loss window): **≤ 5 min**.

**Restore drills**

* **Quarterly** PITR drill; verify app can read restored snapshot in staging.
* **Table‑level point‑restore** rehearsed for donations/refunds.

**AC‑DR‑1:** Restore docs include exact commands and “smoke test” checklist.  
**AC‑DR‑2:** Drill outcomes logged; action items tracked.

## 21.8 Release, rollback & migrations

**Releases**

* CI/CD with **blue‑green / rolling** deploys; health checks; traffic ramp.
* **Feature flags** for risky features; kill‑switches for donations, invites, DMs, email/SMS.

**DB migrations**

* Backward‑compatible; **expand → backfill → contract** pattern.
* Long‑running migrations use **online** strategies; throttled.

**Rollback**

* Code rollback is fast; **migrations** only roll forward (if contract stage removed).
* Config changes audited and revertible.

**AC‑REL‑1:** Each release includes a **runbook link** and rollback plan.  
**AC‑REL‑2:** High‑risk deploys require **IC signoff** if related to checkout/payout.

## 21.9 Security incident response (SIRP)

**Trigger examples:** PII exposure, credential leak, unauthorized access, data tampering.

**Steps**

1. **Declare P0**; form **Security Incident** channel.
2. **Contain:** rotate keys/secrets (7.2), revoke tokens, block malicious IPs/users.
3. **Eradicate:** patch vuln; confirm no lateral movement.
4. **Recover:** restore from known‑good state if needed; validate integrity.
5. **Notify** as required (legal/compliance; user notices per jurisdiction).
6. **Postmortem** with mitigations and deadlines.

**AC‑SEC‑1:** All security events logged; access reviews quarterly; least privilege enforced.  
**AC‑SEC‑2:** Secrets rotated on schedule (90d) and on incident.

## 21.10 Access control & audits

* **SSO + 2FA** for staff (20.A); **step‑up** for dangerous actions.
* **Least privilege** IAM; scoped API keys; IP allow‑lists for webhooks.
* **Quarterly access review**; **joiner/mover/leaver** process within 24h.
* **Audit**: admin actions in admin.audit\_log (who/what/when/IP).

## 21.11 Cost & capacity management

* **Budgets** per provider (Stripe fees observable, SMS/Email volumes, storage/CDN egress).
* **Alerts**: cost anomalies > **30%** day‑over‑day.
* **Capacity**: autoscale policies; load tests before seasonal peaks; DB connection pool sizing.

## 21.12 Data corrections & DSAR runbook

**Data corrections**

1. Open **Case** (Admin).
2. Create SQL fix in **change request**; peer review; run with WHERE id IN (…) protection; snapshot before/after.
3. Post to audit with rationale.

**DSAR**

1. Verify identity → generate export → deliver via secure link.
2. **Anonymize** donor display where allowed; **never** remove financial ledger integrity.
3. Log completion.

## 21.13 Postmortems

* **Blameless**, within **5 business days** for P0/P1.
* Template: Timeline, Customer impact, Root cause (5 Whys), What went well/poorly, Action items (owners, due dates), SLO impact.
* Share summary to stakeholders; internal readout.

## 21.14 Acceptance Criteria (Ops readiness)

* SLOs & dashboards live; alerts route to on‑call; runbooks linked from alerts.
* Status page hooks configured; comms templates available.
* Backups verified; DR drill documented; RTO/RPO achieved in test.
* Release/rollback & migration practices codified in CI.
* Security incident process rehearsed; secrets rotation schedule in place.
* Postmortem cadence established; error budget policy enforced.
* Cost & capacity alerts working.

## 21.15 Quick‑access “Runbooks index” (portal for staff)

A landing page (internal) with cards linking to: **Checkout**, **Webhooks**, **Payouts**, **KYC**, **Notifications**, **DB/Failover**, **Search/Index**, **CMS**, **DM abuse**, **Security Incident**, **Backups/Restore**. Each card shows **last update**, **owner**, **SLOs**.

## 21.16 Roadmap (Ops)

* **Chaos drills**: webhook outage simulator, Stripe sandbox chaos, DB failover game day (quarterly).
* **Error budget automation**: auto‑gating deploys if budget burn > threshold.
* **Automated rollback** on key guardrail violations.
* **Perf budget bots**: PR comments for LCP/CLS/TBT deltas.
* **Synthetic donors**: canary donations with refunds to validate E2E hourly.

# Section 22 — Launch Plan & QA

## 22.0 Purpose & scope

**Goal:** Ship a safe, fast, accessible US‑only fundraising platform with predictable rollout, zero data loss, and clear rollback.  
**Scope:** Environments readiness, data seeding, E2E test matrices (functional, a11y, perf, risk), UAT, go/no‑go checklist, smoke tests, cutover, rollback, and 30‑day hypercare.

**Roles & sign‑offs**

* **Product Owner** — accepts scope; approves go‑live.
* **Eng Lead** — confirms test completion; owns cutover.
* **SRE/IC** — incident commander during launch; owns rollback.
* **Security/Privacy** — approves Section 5 & 6 controls.
* **Payments/Risk** — Stripe/Twilio readiness and thresholds.
* **Support/Trust & Safety** — KB complete; macros live; moderation SOPs ready.
* **Marketing/CMS** — public copy, OG, sitemaps, redirects ready.
* **Legal** — legal pages (two‑person approval) published.

**Exit criteria headline**

* **No open P0/P1**; ≤ **5 open P2** (documented workarounds), 0 known data corruption paths.
* All **performance budgets** (Section 4.6) green on target pages.
* All **WCAG 2.2 AA** critical paths pass manual & automated checks.
* **Stripe/Twilio** webhooks verified & observed in staging.
* **Admin safety rails** (feature flags, kill switches) validated.

## 22.1 Environments & cutover prerequisites

**Environments**

* **Sandbox/Staging/Prod** isolated; unique keys; obvious banners in Admin & portal.
* Infrastructure: blue/green or rolling deploy ready; database backups (PITR) enabled and tested (Section 21.7).

**Before code freeze**

* ✅ Stripe: Payments, Identity, Connect accounts configured; Apple Pay/Google Pay domains verified; Radar rules aligned to Section 5.
* ✅ Twilio: A2P 10DLC registration complete; Verify service id configured; STOP/HELP responses tested.
* ✅ Email: SPF/DKIM/DMARC live; bounce/complaint webhooks confirmed.
* ✅ CDN/Storage: S3 buckets, AV scan, CloudFront; signed URLs.
* ✅ Address: USPS/Smarty keys; address autocomplete on profile & rewards claim.
* ✅ IRS badge (if used day‑1): aggregator key; monthly cron.
* ✅ CAPTCHA: hCaptcha site/secret keys wired where specified.
* ✅ OAuth (Apple/Google) if enabled: bundle ids & redirect URIs registered, private keys stored.
* ✅ DNS & TLS: prod domains & wildcard certs; HSTS.
* ✅ Analytics: first‑party event pipeline; optional GA/Posthog honoring consent.

**Data seeding**

* Categories (12), default tip/fee config, discovery ranking defaults, report reasons, copy library, email/SMS templates v1, OG image templates, KB index skeleton, feature flags defaults (off unless specified), marketing CMS initial content (Home, About, Contact, KB shells, Legal pages).

## 22.2 Test strategy & matrix (MVP + critical edge cases)

**Format below:** Area → Scenarios → Key checks. Use it as a master checklist (traceability back to sections is noted in [brackets]).

### A) Identity, Auth & Account (Reg → Login → Security)

1. **Registration (phone‑first)** [10, 11, 18]
   * Phone OTP: correct/fail/expire; resend; voice fallback.
   * Email verify link: one‑time; expired; replay safely no‑ops.
   * Accessibility: OTP “six boxes” + single‑field fallback reads properly.
2. **Login & sessions**
   * New device alert; 2FA code via SMS (STOP/HELP honored).
   * Session cap = **1 active session** (your choice); force logout on second login.
3. **Security changes**
   * Email change with confirm link; phone change with OTP; **24h payout cooldown** banner in Wallet.

### B) Verification (KYC/KYB) [11]

* ID capture: pass; 3× fail → manual review; selfie required by risk.
* SSN last‑4 (individual) vs EIN (org); bank account add; name mismatch → **Compliance Hold**.
* Publish gate: Email/Phone/ID green; Payout gate: SSN/EIN + Bank green.

### C) Campaign Creation & Team [12]

* Wizard:
  + Page‑1 basics: goal ≥ $100; deadline 4–12 wks; city/state US‑only; AoN toggle if allowed; cannot change AoN after publish.
  + Page‑2 story: sanitize links; 20k soft cap; 30k hard block.
  + Page‑3 media: 16:9 cover required; ≤15 images (≤5 MB) & ≤5 videos (≤100 MB); alt text required.
  + Page‑4 tiers: ascending rule; quantity caps; physical vs digital; shipping required toggles flows.
  + Review & Publish: all checks green; blocked if ID not verified.
* Team: invite (new user vs existing), single‑use link 7 days; seat cap 5; co‑lead = 1; leaderboard toggle.

### D) Public Campaign Page [13]

* Header badges; AoN tooltip; progress module; team leaderboard.
* Donate widget: min $5; whole dollars; soft guardrail at high amounts; **COI** block for members/support; organizer self‑donation allowed & flagged.
* State banners: Live / Paused (under review) / Ended KWR / AoN not funded; Donate disabled when appropriate.
* Gallery a11y: keyboard nav; no autoplay; lightbox focus trap.

### E) Checkout & Payments [14, 7]

* Quick chips + custom amount; tip; cover fees; terms required.
* 3DS flows (frictionless & challenged); recover gracefully to confirmation.
* AoN copy at checkout & receipt; KWR normal copy.
* Error handling: retry once; card declines; non‑US card allowed; prepaid limited.
* Donor privacy: hide name publicly vs fully anonymous (blocks reward claim).

### F) Rewards (Claim → Fulfillment) [12]

* Donor claim page: ship/no‑ship; US address validation; options (Size S/M/L).
* Claim abandon → persistent banner; edit until organizer sets “Pending”.
* Organizer fulfillment table: bulk status updates; tracking number validation; donor‑visible note.
* Nudges at 14/30/45 days; escalation at 45.

### G) Wallet, Payouts & Finance [10.D, 15, 20.D]

* Balance math = sum of succeeded (net) − prior payouts; refunds decrement.
* Payout eligibility: after campaign end + 3–5 business days hold; SSN/EIN/Bank verified; no hold flags.
* Payout lifecycle: requested → in\_review (dual‑approval for high value) → processing → paid or returned (notifications & voice fallback).
* Returned payout triggers banner + email/SMS; resubmit after bank update.

### H) Refunds & Disputes [14.L, 20.E, 7.4]

* Donor opens request; Organizer/Admin approves/declines with reason; partial refunds update receipt.
* AoN auto‑refund at deadline; donation status aon\_auto\_refunded.
* Stripe disputes intake; evidence kit assembled; deadlines tracked; outcomes mirrored.

### I) Discovery, Search & SEO [16, 9]

* Search facets + sort; suspended hidden; ended campaigns only shown when filter enabled.
* Cards show chips (Trending, Ending soon, Editor’s Pick) & badges.
* Home modules reorder; “In your state” consent flow.
* Sitemaps; canonical tags; OG images; 410 vs noindex policies.

### J) Notifications & Messaging [18, 10.S]

* Routing matrix honored (email/SMS/voice/in‑app); quiet hours except security/critical finance.
* Batching for organizer donation summaries; idempotency keys.
* DM: new thread limits; mute; report to moderation; donor‑only mode toggle.

### K) Admin Console (Trust & Safety, Finance, CMS, Feature Flags) [20]

* Moderation actions: soft warning; suspend/unsuspend; require edits; content removal with evidence.
* Finance Ops: returns, negative balance, reserves, dual‑approval thresholds.
* Template Manager: versioned email/SMS; test send; variables validated.
* Config & Feature Flags: donation kill‑switch; DM off; invites off; discovery weights; redirects.

### L) Privacy, DSAR & Retention [6]

* Cookie banner flows; GPC honored; Do Not Sell/Share persists.
* DSAR export & delete/anonymize path; SLA timers; audit trail.
* Nightly purge jobs (dry‑run in staging).

### M) Risk & Abuse [5]

* Velocity limits (3/min, 10/hour) show friendly blocks; CAPTCHA at thresholds.
* High‑amount step‑ups; prepaid limits; non‑US with extra screening.
* COI donation block for team members; organizer self‑donations flagged.
* Lists (deny/allow/gray) matter; simulation tool.

**Evidence for each scenario**

* Screenshot or screen recording, test user ids, timestamps, logs/traces ids, and resulting DB ids.

## 22.3 Accessibility QA (focused)

* **Manual**: keyboard‑only Donate (campaign → checkout → confirmation), OTP flow (registration & phone change), reward claim, payout request; NVDA/VoiceOver reads labels & errors correctly.
* **Automated**: axe‑core CI (no high severity); Lighthouse ≥ 90 Accessibility on Home, Search, Campaign, Checkout, Portal Profile.
* **Color/contrast**: chips, buttons, progress bars meet ratios; prefers‑reduced‑motion disables animations.

## 22.4 Performance & load tests

* **Web Vitals** on device lab (mid‑range Android over 4G): budgets from Section 4.6.
* **Checkout latency** P95 ≤ 4s; **Webhook** P99 ≤ 60s (stripe → DB).
* **Load**: simulate **peak** (e.g., 100 RPS public browse, 10 RPS checkout starts, webhook storm 2× normal) for 30 min; error rates < 0.5%, no data loss.
* **Warm cache** scenarios: verify LCP after first/second load.

## 22.5 Security checks (baseline)

* CSRF on forms; CORS locked down; HSTS enabled.
* IDOR probes on portal/admin routes; RLS rules verified by tests.
* Headers: CSP (allow Stripe/Twilio endpoints), X‑Content‑Type, X‑Frame‑Options/SameSite cookies.
* Rate limits & CAPTCHA at auth, contact, report, DM new thread.
* Secrets: env‑only; rotation schedule; no secrets in client bundles.

## 22.6 UAT plan (role‑based scripts)

**Participants & accounts**

* Donor, Organizer (individual), Org Admin (nonprofit), Team Co‑Lead/Member, Campaign Support, Moderator, Risk Analyst, Finance Ops, Support Agent, Super Admin.

**UAT flow overview (condensed)**

1. **Organizer** verifies ID, builds a KWR campaign, uploads media, creates tiers, invites teammates, publishes.
2. **Donor A** donates preset $50 (KWR), hides name, claims digital reward.
3. **Donor B** donates $1000 (triggers 3DS), claims physical reward; edits address before Pending.
4. **Organizer** bulk‑marks Pending, adds tracking, sends donor note; Nudges verified by time travel in staging.
5. **Team Member** shares referral link; donation attributed; leaderboard updates.
6. **Moderator** suspends & unsuspends; requires edits; checks public states.
7. **Organizer** ends campaign; Wallet shows balance; requests payout; Finance dual‑approves; payout paid; statement exported.
8. **Donor** requests partial refund; Organizer approves; receipt updated.
9. **Support** handles ticket via Contact form; status syncs.
10. **Legal** publishes updated Privacy; two‑person approval; version history visible.

**UAT acceptance:** Each step gets **pass/fail**, evidence link, blocker severity, owner, fix date.

(Appendix A includes step‑by‑step UAT scripts you can copy into your tracker.)

## 22.7 Go/No‑Go checklist (final 48h → T−0)

**T−48h**

* Code freeze; only hotfixes via change control.
* Staging green: all test suites pass; perf & a11y within budgets.
* Content freeze: Home, Legal, KB finalized.
* On‑call roster & incident channels set; statuspage messages templated.
* Backups verified; restore drill recently passed.
* Feature flags staged: **donations OFF**, **DM ON**, **invites ON**, **discovery ON**, **notifications ON**, **payouts LOCKED**.

**T−24h**

* DNS TTL lowered (if applicable).
* Stripe/Twilio/SendGrid webhooks pointing to **prod** (shadow mode allowed where safe).
* Admin staff accounts provisioned; SSO + 2FA verified.
* Helpdesk macros live; Support training complete.

**T−2h**

* Deploy prod; run **smoke tests** (see 22.8).
* Turn **donations ON** behind flag but **hidden** (test via hidden route).
* Verify event bus → notifications → inbox delivery attempts.

**T−0 (Launch)**

* Remove “hidden” gates; open public routes.
* Announce internally; start hypercare war‑room.

**No‑Go triggers**

* Any P0; sustained checkout success rate < 99%; webhook backlog P99 > 5 min; payout failures > 5% on test payout; legal/PII defect.

## 22.8 Production smoke tests (15–20 minutes, post‑toggle)

1. **Public**
   * Home loads ≤ 2.5s LCP; Search returns results; one category page paginates.
2. **Campaign**
   * Create minimal KWR campaign (private slug), publish; verify card on discovery.
   * Donate $5 with test card token (Stripe live micro charge); receipt email arrives; in‑app noti appears.
3. **Rewards**
   * Donation ≥ Tier 1; claim digital; Organizer marks Pending → donor email.
4. **Notifications**
   * Trigger KYC verified (admin stub) → email arrives; SMS test (payout returned template) to verified Twilio number (STOP/HELP responses OK).
5. **Admin**
   * Suspend test campaign → public banner shows; unsuspend.
6. **Finance**
   * Initiate **$1** test payout (safe destination) → observe status change to processing; cancel if your provider allows test payout; otherwise use Connect test environment (if running a “dark launch” seed account).

**Record:** timestamps, IDs, delivery logs, and screenshots.

## 22.9 Cutover & rollback

**Cutover pattern**

* Use **feature flags** to progressively enable: discovery → donations → DM → invites → payouts (after first end‑of‑day).
* Keep **read‑only mode** switch handy (donations OFF, payouts OFF, CMS legal only).

**Rollback decision matrix**

* **Checkout broken / payment provider outage** → Donations OFF; show banner; keep browsing; re‑enable after fix.
* **Webhook processing stuck** → Keep donations ON (idempotent) if DB writes healthy; fix consumers; if DB unhealthy → set read‑only; pause donations temporarily.
* **Payout pipeline unhealthy** → Payouts OFF; notify organizers; funds safe in balance.
* **Security incident** → Follow Section 21.9; rotate keys; statuspage; decide on temporary shutdown.

**Rollback mechanics**

* **Code**: revert to last green release via deploy tool.
* **Config**: flags revertible instantly; admin edits logged.
* **DB**: **do not** roll back schema; use forward‑fix; for corrupt rows, run targeted migrations with audit.

## 22.10 Hypercare (Day 0–30)

**War‑room cadence**

* **D0–D3:** 24×7 coverage; stand‑ups every 4h; dashboards on wallboard.
* **D4–D14:** business hours + on‑call overnight.
* **D15–D30:** normal on‑call; weekly review.

**KPIs to watch (with thresholds)**

* Payment success rate ≥ 99.9%; 3DS challenge rate within expected bounds.
* Webhook age P99 ≤ 60s; DLQ = 0.
* Refund rate & dispute opens (daily).
* Payout failures/returns < 2%.
* SMS DLR ≥ 98% on OTP/critical; email bounces < 0.5%.
* Error logs & 5xx rates stable.
* Page Web Vitals trending (LCP/CLS/TBT) within budgets.
* Search index freshness ≤ 15 min.

**Comms**

* Internal daily digest to stakeholders (donations, active campaigns, issues).
* External: statuspage when applicable; marketing comms per plan.

**Post‑launch**

* **D+7**: mini‑postmortem of launch; backlog grooming.
* **D+30**: full retrospective; convert learnings into standards.

## 22.11 Documentation & training

* **Support playbook**: refund policy nuances (AoN vs KWR), reward status questions, identity troubleshooting, payout holds, donor privacy options.
* **Moderation SOP**: evidence handling, suspend/require‑edits workflow, donor‑only report intake.
* **Finance runbook**: payouts, returns, reserves, negative balance handling.
* **Risk analyst guide**: queues, thresholds, lists, dual‑approval.
* **Admin CMS guide**: publishing/rollback; OG templates; redirects.

All docs linked from an internal “Runbooks Index” (Section 21.15).

## 22.12 Acceptance Criteria (launch readiness)

* Test matrix executed with evidence; **traceability** to every major requirement in Sections 4–21.
* Accessibility audits passed; known minor issues tracked with deadlines.
* Performance budgets measured & met in staging and canary prod traffic.
* Observability & alerts firing (synthetic canary donations hourly).
* Webhooks verified end‑to‑end with idempotency; DLQ empty.
* DSAR export/delete flows tested; cookie/GPC honored.
* Admin safety rails validated (kill switches, flags, dual‑approvals).
* Go/No‑Go completed; all owners signed off.

## Appendix A — UAT script templates (copy/paste)

**Template fields:** Scenario, Role, Preconditions, Steps, Expected, Evidence, Pass/Fail, Notes, Owner.

**Sample: Donation (AoN, 3DS)**

* **Role:** Donor
* **Pre:** Live AoN campaign ending in ≤ 2 days; $100 goal; preset chips visible.
* **Steps:** Open campaign → select $100 → toggle cover fees ON → proceed to checkout → complete 3DS challenge → confirm.
* **Expected:** Receipt email; donation listed in Donor history; AoN caution shown; Organizer sees donation; progress updated live.
* **Evidence:** Screenshot of confirmation, email header, donation id, trace id.
* **Pass/Fail:** \_\_\_ Notes: \_\_\_ Owner: \_\_\_

**Sample: Organizer payout (returned)**

* **Role:** Organizer + Finance Ops
* **Pre:** Campaign ended; balance ≥ $50; bank intentionally incorrect (staging).
* **Steps:** Request payout → Finance approves → provider returns payout.
* **Expected:** Organizer gets SMS+email; Wallet shows returned status & banner; Finance queue shows case; resubmit after bank update.
* **Evidence:** Logs, screenshots, payout id.
* **Pass/Fail:** \_\_\_ Notes: \_\_\_ Owner: \_\_\_

## Appendix B — Production smoke test script (copy/paste one pager)

1. Home loads (LCP time, CLS).
2. Search “medical” → open first campaign.
3. Donate $5 (real charge to card you’ll refund) → confirm receipt.
4. Claim digital reward (if tiered) → organizer marks pending.
5. Suspend test campaign; verify banner; unsuspend.
6. Trigger one payout event (test scope) or verify Connect webhooks by simulating in sandbox link.

## Appendix C — Comms templates

**Internal launch note (Slack/email):**  
“Launching today at {time}. Flags: discovery ON, donations ON at T+15m, payouts locked until EOD. War‑room: {link}. On‑call: {IC name}. KPIs: {dashboard link}.”

**Public status (if needed):**  
“We are rolling out a new version of our site today. Some features may be temporarily limited between {start} and {end}. Thanks for your patience.”

# Section 23 — Support & Helpdesk UX

**Scope:** End‑to‑end customer support for donors, organizers, org admins, team members, and guests; staff helpdesk workflows; AI chatbot; portal “My Tickets”; ticket data model; macros/templates; SLAs; routing; moderation & finance handoffs; compliance.

**Depends on:** §5 (Risk/Abuse), §6 (Privacy/Retention), §7 (APIs/Webhooks), §8 (Schema), §9 (KB/CMS), §10 (Portal), §12–15 (Campaign/Rewards/Checkout/Payouts), §17 (DM → ticket), §18 (Notifications), §20 (Admin Console), §21–22 (Ops/QA).

## 23.0 Principles

1. **Solve fast, safely.** Sensitive actions (refunds, payouts, KYC) require verified login and role checks.
2. **Channel the right way.** Self‑serve and KB deflection first; then DM when contextual; then ticket; phone for urgent only.
3. **Single source of truth.** Every case is a **ticket** with audit trail, attachments, and linked entities (user, campaign, donation, payout).
4. **Respect privacy.** Never ask for SSN over support; mask payment details; redact automatically.
5. **Observable.** SLAs, backlog, and CSAT are measurable; escalations are explicit.

## 23.1 Channels & entry points

**Public/Marketing site**

* **Contact form** (/contact; §9.4.3): creates ticket (topic‑routed). hCaptcha + rate limits; guests allowed but sensitive requests auto‑require login to continue.
* **KB widgets** (article bottom “Still need help?”): opens prefilled **Ticket modal** with article context.

**Portal**

* **Support (left nav)**: “My Tickets” + “New request” (dynamic form).
* **Contextual “Get help”** buttons:
  + Donation receipt page → “Receipt problem”
  + Rewards page → “Reward missing/damaged”
  + Wallet/Payouts page → “Payout returned”
  + Verification page → “Trouble verifying ID”  
    These open the **New request** form **pre‑contextualized**.

**DM → Ticket**

* From any DM (Section 17), **“Convert to ticket”** (organizer or staff). Thread transcript is attached; future replies continue in ticket.

**Email**

* **inbox@{brand}.com** general intake; **support@{brand}.com** replies only.
  + Auto‑acknowledge; parse from: → map to user/contact.
  + If unknown/guest: ticket created with “Unverified email” flag; ask them to sign in to continue for sensitive actions.

**Phone**

* Single number with IVR **topic selection** (Donor, Organizer, Payouts, Safety).
* Call logging screen for agents; callback & voicemail options (business hours only).
* Identity verification script before account‑specific discussion.

**AI Chatbot (web widget + portal)**

* **Front‑door deflection**: answers from KB & policy corpus; can **create a ticket** with the transcript and selected category.
* **Guardrails:** never take payments, never collect SSN, never promise refunds/payouts—only guide.

## 23.2 Ticket types & dynamic forms (what we collect)

“Dynamic forms” = different fields per topic, with validations & hints. Where a **sensitive action** is requested, require **login** and **role checks**.

### A) Donor topics

1. **Receipt & donation proof**
   * **Fields:** campaign URL/ID (auto if from context), approximate date/time, amount, last‑4 card (optional), email on receipt.
   * **Outcome:** resend receipt; fix email on donor profile (after verify); attach receipt PDF.
2. **Refund request**
   * **Fields:** donation ID (required; pick from history), reason (dropdown + free text), amount (default full; allow partial).
   * **Gate:** logged‑in **donor** role only.
   * **Outcome:** creates **refund review** task for Organizer (or Admin). Copy re‑states policy that only Organizer/Admin can execute refunds.
3. **Reward issue (missing/damaged/wrong)**
   * **Fields:** donation ID (required), tier, shipping address confirm, photo upload (≤3), desired resolution (resend/refund/other).
   * **Outcome:** notifies Organizer; links to Reward row; SLA (14d initial, 30d escalation).
4. **Payment problem (charge failed/3DS/duplicate)**
   * **Fields:** last 4 digits, bank name (optional), timestamp, screenshot (optional).
   * **Outcome:** check payment logs; educate; issue refund if duplicate validated by logs (Organizer/Admin only).

### B) Organizer/Org Admin topics

1. **Identity/KYC/KYB**
   * **Fields:** which step failed (ID, SSN, EIN), error code (if shown), photos (ID edges visible).
   * **Outcome:** KYC retry tips; manual review queue if 3× fails.
2. **Payouts (status/returned)**
   * **Fields:** payout ID (select), bank last‑4 (masked), account holder name (text), return code if present.
   * **Outcome:** **Finance Ops queue**; block until bank updated; trigger resubmit.
3. **Campaign moderation / policy**
   * **Fields:** campaign ID, requested change (deadline extension KWR, content edit requests), reasoning.
   * **Outcome:** **Moderation case link**; possible suspend/require edits; commit change if allowed.
4. **Team & invites**
   * **Fields:** campaign ID, invited email, error message/expired link.
   * **Outcome:** resend invite; extend expiry; audit log note.
5. **Technical issue / bug**
   * **Fields:** URL, steps to reproduce, browser/OS, screenshot.
   * **Outcome:** triage to engineering; link to bug tracker.

### C) Safety & legal

1. **Report a campaign** (donors‑only)

* Uses **Report** flow (§13.11) → creates **Moderation case**, not a normal support ticket.
* Support tickets that arrive about safety are **linked** to the mod case.

1. **Privacy & DSAR**

* **Fields:** type (access/export/delete), identity verification steps, scope.
* **Outcome:** privacy workflow (Section 6).

**Common fields on all forms:** Priority (auto), Preferred contact method, Attachments (≤5, images/PDF only), Consent checkbox for data processing.

## 23.3 Roles, queues & permissions (ties to §20)

**Roles**

* **Support Agent:** handle tickets; add internal notes; trigger predefined actions (receipt resend, invite resend); cannot refund/payout.
* **Support Lead:** all of above + reassign, merge, bulk actions, SLA overrides.
* **Moderator (T&S):** owns moderation cases; can pull linked tickets.
* **Finance Ops:** owns payout/negative balance queues; can mark returned/paid; cannot alter campaign content.
* **Risk Analyst:** sees fraud flags; can request additional verification; set holds.
* **Super Admin:** all permissions + template/config management.

**Queues (views)**

* **New**, **In Progress**, **Waiting for Customer**, **Pending Third‑Party**, **On Hold (Compliance)**, **Resolved**, **Closed**, **SLA at risk**.
* **Specialized queues:** **Payouts**, **KYC/KYB**, **Refund reviews**, **Safety/Moderation**, **DM‑converted**.

**PII access**

* Email/phone visible to staff; **full card never** visible; **last‑4** only from payment logs.
* SSN/EIN **never** requested or stored in ticket; if a user shares, **auto‑redact** to \*\*\*‑\*\*‑1234 on save.

## 23.4 Routing, SLAs & escalations

**Auto‑routing rules**

* Topic → Queue + **Assignee group** (Support vs Finance vs Mod).
* Organizer vs Donor inferred by login; Org Admin flagged.
* Language/region (US‑only MVP): set timezone → SLA clock.

**SLA targets (business hours Mon–Fri, 9a–6p local; holidays configurable)**

* **P0 Critical** (payout returned for large amount; security incident): First reply **<1h**, resolution **same day**.
* **P1 Urgent** (payout returned, KYC block after attempts, duplicate charge, AoN refund issue): First reply **<4h**, resolution **1–3 days**.
* **P2 Normal** (reward issues, receipt questions, team invites): First reply **<1 business day**, resolution **3–5 days**.
* **P3 Low** (how‑to, feature requests): First reply **<2 business days**, resolution **as capacity**.

**Escalations**

* If **Waiting for Customer** > 7 days → auto‑reminder; **+7 days** → auto‑close with reopen link.
* SLA breach approaching: **SLA at risk** view + orange badge; breach → red badge + Slack alert (internal).

**Collision detection**

* Warn if multiple agents open same ticket; show presence indicators; lock on reply compose.

## 23.5 Macros & snippets (starter library)

All macros render **friendly, plain English**, with links into KB where applicable. Agents can insert variables ({first\_name}, {campaign\_title}, {donation\_id}, etc.).

**Donor**

* **Receipt resend**
* **Refund policy explainer** (AoN vs KWR; organizer/admin authority)
* **Reward claim reminder** (link to claim page)
* **3DS help** (bank confirmation steps)

**Organizer**

* **KYC retry tips** (lighting, edges, no glare; clear image)
* **Returned payout** (how to update bank; why returns happen; next steps)
* **Team invite expired** (how to regenerate)
* **Moderation require‑edits** (policy references)

**General**

* **We need more info** (list of items + how to collect safely)
* **Closing due to inactivity** (with reopen instructions)

## 23.6 AI chatbot (triage & handoff)

**Capabilities (MVP)**

* Answer FAQs from KB (§9) and policy pages (ToS/Privacy/Refunds/Community).
* Walk through simple flows (find a receipt; how to claim rewards; how to verify ID).
* **Escalate** to ticket on triggers: payout/finance, refund request, ID verification failures, harassment/fraud claims, anything the bot is unsure about after 2 exchanges.

**Guardrails**

* Never ask for or accept **SSN**, **full card number**, **bank login**, or **photo IDs**.
* When asked about refunds/payouts: bot **explains policy** and **offers to create a ticket** (no promises).
* Include persistent **handoff button** “Connect me to a person.”

**Handoff**

* Creates ticket with **bot transcript**, user’s topic selection, and context IDs (campaign/donation/payout).
* Sets expectation: “We’ll reply within {SLA}.”

## 23.7 User‑facing: “My Tickets” (portal)

**List view**

* Columns: Ticket ID, Subject, Category, Status (New/In progress/Waiting/Resolved/Closed), Last updated, Priority badge, Linked campaign/donation.
* Filters: Status, Category, Date range. Search: Subject/ID.
* CTA: **New request** (opens dynamic form).

**Detail view**

* Header: Title, Status, Priority; linked entities chips.
* Thread: Messages (agent/customer), internal notes **hidden from user**; attachments preview; timestamps.
* Composer: text (2000 chars), image/PDF attachments (≤5, 8MB each).
* Actions: **Add info**, **Close request** (with comment), **Reopen** (within 14 days).
* **CSAT** pops after agent marks Resolved (see §23.12).

**A11y**

* Keyboardable thread; SR announces agent/customer and time; file inputs labelled.

## 23.8 Agent console (helpdesk UX)

**Core panes**

* Left: Views/Queues, saved searches, bulk actions.
* Center: Ticket thread with composer; macros; attachments; **Internal note** vs **Public reply** toggle.
* Right: Context panel with **User card** (roles, verification status), **Campaign card**, **Donation card**, **Payout card**; SLA timers; tags; history.

**Key actions**

* Assign/mention teammates (@); set priority; add tags; merge/split tickets; link to moderation case; convert DM ↔ ticket; trigger **receipt resend**, **invite resend**; open **refund review** action (does **not** execute refund).
* **Shortcuts:** R reply, N internal note, A assign, E apply macro, C close.

**Safety**

* Redaction on paste (detect 9‑digit patterns/16‑digit patterns); mask automatically; warn agent.
* Attachment AV scan & type restrictions (images/PDF only by default).

**Audit & training**

* Every agent action logged; transcript export for training; per‑agent stats visible to Support Lead.

## 23.9 Notifications (ties to §18)

**User**

* Ticket created, agent replied, waiting‑for‑you reminder (after 72h), resolution, closed, CSAT survey. Channels: Email + In‑app; SMS **off** by default (opt‑in per topic).

**Agent**

* New assignment, @mention, SLA at risk. Channels: In‑app + Email (digest optional).

**Templates**

* Reside in **Admin Template Manager** (§20.H) with variables validation.

## 23.10 Integrations & data model

**Helpdesk vendor**

* Use a modern helpdesk (e.g., Zendesk/Help Scout/Freshdesk) **or** build light in‑house. Either way:
  + **Webhooks** for ticket opened/updated/closed, comment added, assignment changes.
  + **SSO** for agents (SSO + 2FA; §20.A).
  + **Data residency** US; retention configurable (see §6).

**Data model (adds to §8)**

support.ticket

- id, requester\_user\_id nullable, requester\_email, subject, category, subcategory, status

('new','in\_progress','waiting','pending\_third\_party','on\_hold','resolved','closed'),

priority ('p0','p1','p2','p3'), queue ('general','payouts','kyc','refunds','moderation',...),

linked\_entities jsonb [{type:'campaign'|'donation'|'payout'|'dm\_thread', id}],

tags jsonb[], sla\_first\_response\_at, sla\_due\_at, last\_public\_update\_at,

created\_at, updated\_at, closed\_at, csat\_score nullable, csat\_comment

support.message

- id, ticket\_id, sender\_user\_id nullable, sender\_role ('user','agent','system'),

body\_text, attachments jsonb[], is\_internal\_note bool, created\_at

support.attachment

- id, ticket\_id, message\_id, file\_ref, mime, size\_bytes, scan\_status

support.sla

- id, ticket\_id, severity, first\_response\_target\_at, resolve\_target\_at, paused bool, paused\_reason

support.csat\_event

- id, ticket\_id, sent\_at, responded\_at, score (1–5), comment, channel

support.email\_log

- id, ticket\_id, provider, msg\_id, status, created\_at

support.phone\_log

- id, ticket\_id, call\_sid, from\_e164, duration\_sec, recording\_ref?, disposition ('answered','voicemail','missed'), created\_at

## 23.11 Security, privacy & compliance

* **Auth required** for sensitive topics; guests limited to general inquiries.
* **Never** ask for or store **full card**, **SSN**, **driver’s license images**.
* **Auto‑redaction** on inbound: patterns for SSN/CC; strip EXIF metadata from images.
* **Retention:** tickets/messages kept **24 months**, attachments **12 months** unless legal hold (see §6.7).
* **Access control:** Agents see only what they need; Finance queue restricted; Mod queue restricted.
* **Export (DSAR):** support transcripts included; internal notes excluded unless legally required.
* **Call recording:** Off by default for MVP; if enabled later, get **explicit consent** and store retention/purge policy.

## 23.12 Metrics & dashboards (day‑1)

**Core KPIs**

* **FRT** (first response time) by topic & channel
* **MTTR** (median time to resolve) by topic
* **Backlog** by status and SLA risk
* **Reopen rate**
* **Deflection rate** (KB views → ticket creation ratio)
* **CSAT** (1–5) post‑resolution; optional smiley 3‑point for SMS
* **Topic distribution** (top issues)
* **Escalation ratio** (to Finance/Mod/Risk)
* **Refund request outcomes** (approved/declined; driver analysis)

**Reports**

* Weekly digest to stakeholders; CSV exports; “Custom report builder” (from §20.R) supports Support data.

## 23.13 Wireframe callouts (hand‑off to design)

### A) ****Portal → Support → My Tickets (desktop)****

1. **Header**: “Support” <h1> with “New request” primary button.
2. **Tabs/Filters**: All / Open / Waiting / Resolved / Closed; search box with placeholder “Search subject or ticket #”.
3. **Table**: columns—ID (link), Subject, Category chip, Status pill, Last updated (relative), Linked (campaign/donation icons), Priority badge.
4. **Empty state**: illustration + “No tickets yet. Try the Knowledge Base or open a new request.”
5. **Row click → Detail**: see §23.7.

### B) ****New request (dynamic form modal/page)****

1. **Category select** (icons): Donations, Rewards, Payouts, Verification, Team & invites, Technical, Privacy.
2. **Form body** loads with relevant fields + context chips (e.g., “Donation: {id}”).
3. **File uploader**: drag‑drop or browse; accept images/PDF; size cap; AV scanning.
4. **Consent** checkbox: “I agree not to share sensitive info (SSN, full card numbers) here.”
5. **Submit** CTA; success screen with ticket # + “View ticket”.

### C) ****Agent console — ticket detail****

1. **Title line** with emoji category icon, ID, Status dropdown, Priority dropdown.
2. **Context panel (right)**: User card (roles, verified badge), Campaign card (status), Donation/Payout chips with statuses; SLA timer (countdown).
3. **Thread**: alternating bubbles; internal notes styled differently; attachments inline thumbs; redaction alerts if PII detected.
4. **Composer**: Public/Internal toggle; macros menu; quick actions (receipt resend, invite resend); “Convert to moderation” and “Finance handoff” buttons.
5. **Presence indicators** show who else is viewing.

### D) ****AI Chatbot widget****

1. **Launcher** bottom‑right; header “Ask a question”.
2. **Suggested prompts**: “Find my receipt”, “How do refunds work?”, “Update bank details”, “Trouble verifying ID”.
3. **Handoff** button visible; “Create a ticket” summary step showing what will be sent.

## 23.14 Edge cases & rules

* **Guest requests refund:** Reply requires **login**; provide link; ticket remains “waiting” 7 days then auto‑close.
* **Organizer asks to delete donor data via ticket:** redirect to **Privacy/DSAR** flow; do not action manually.
* **Donor claims fraud (card stolen):** instruct to contact bank; also open **Risk** case; mark donation disputed/flagged.
* **Harassment in messages:** convert to ticket + **Moderation** with attached evidence; mute/block guidance to user.
* **Multiple tickets same issue:** merge with note; preserve newest as master; notify requester.
* **Language barriers:** English‑only MVP; provide simple copy templates; consider translate assist Phase‑2.

## 23.15 Acceptance Criteria (summary)

1. **Multi‑channel intake** works: Contact form, Portal request, DM→Ticket, Email intake, AI handoff, Phone log.
2. **Dynamic forms** collect correct fields; sensitive topics require login & role checks.
3. **Routing** maps topics to queues with SLA timers; **SLA views** highlight “at risk”.
4. **Agent console** supports replies, internal notes, macros, assignments, merges/splits, redaction, and context linking (user/campaign/donation/payout).
5. **Users** can view, reply, attach, close, and reopen tickets in the portal; CSAT sent on resolve.
6. **Notifications** (email/in‑app) fire on create, reply, waiting reminders, resolution, close; respect preferences & quiet hours (§18).
7. **Security & privacy**: no SSN/CC stored; attachments scanned; retention enforced; staff access audited.
8. **Integrations**: webhooks idempotent; helpdesk SSO; errors surface in Admin health panel.
9. **Metrics**: dashboards show FRT/MTTR/backlog/CSAT; exports available.

## 23.16 QA checklist (tie to §22)

* Create tickets from: Contact form, Portal form (contextual), Email, DM convert, AI handoff.
* Refund request: donor only; organizer/admin approval path; receipt updates.
* Payout returned: routes to Finance; SMS/voice fallback to organizer (from §18) triggered by Finance state.
* KYC failure: retry tips macro; manual review flag path.
* SLA timers & breach alerts; “Waiting for customer” reminders; auto‑close with reopen link.
* Agent console: macros, internal notes, redaction on PII, attachments AV scan.
* Merge/split tickets; link to campaign/donation/payout; convert to moderation case.
* Portal “My Tickets”: list, filters, detail, reply, close, reopen; CSAT capture and reporting.
* Notifications: create/reply/reminder/resolution flows; preferences/quiet hours honored.
* Data retention purge jobs (dry‑run) and DSAR export.
* Analytics events logged for support funnels.

## 23.17 Microcopy kit (ready to ship)

* **Contact success:** “Thanks! We’ve created ticket **#{id}**. We’ll reply by **{sla\_window}**.”
* **Refund policy (donor):** “Refunds are approved by the organizer or our team after review. We’ll take a look and follow up.”
* **Sensitive info warning (form):** “For your safety, don’t share SSNs or full card numbers. We’ll never ask for them.”
* **Waiting reminder:** “We’re waiting on your reply to **#{id}**. Reply within 7 days or we’ll close this for now.”
* **Auto‑close:** “We haven’t heard back, so we’ve closed **#{id}**. You can reopen it anytime within 14 days.”
* **Payout returned (organizer):** “We couldn’t deliver your payout. Update your bank details to try again.”
* **KYC retry:** “Let’s try again—use a well‑lit area, remove cases, and fit all 4 corners of your ID.”
* **CSAT:** “How did we do? Rate your experience for **#{id}**.”

## 23.18 Roadmap (Phase‑2)

* **In‑product chat with human agents** (handoff from bot), with presence and typing indicators.
* **Multilingual support** (machine‑assisted, agent‑verified).
* **Call recording + transcripts** with consent; sentiment & topic detection.
* **Proactive support** (detect bounced payouts or failed KYC and open tickets automatically).
* **Support knowledge suggestions** for agents (AI recommended macros).
* **Customer portal for orgs** with **org‑wide ticket view** (aggregate across staff).

# Section 24 — Payouts Pipeline

**Scope:** End‑to‑end payouts for US‑only organizers and nonprofits: eligibility gates, accrual math, reserves/holds, scheduler & batching, Stripe execution, returns/retries, negative balances, statements/reconciliation, roles/approvals, instrumentation, wireframes, AC & QA.

**Depends on:** §2 (Economics), §3 (Roles), §5 (Risk), §6 (Privacy/Retention), §7 (APIs/Stripe), §8 (Schema), §10.D (Wallet), §11 (KYC/KYB), §12 (Campaign lifecycle), §14 (Checkout/Refunds), §18 (Notifications), §20 (Admin/Finance Ops), §21–22 (Ops/Launch).

**Defaults honored from earlier decisions:**

* **Payout timing:** On campaign end + **3–5 business days** hold.
* **Minimum payout:** **$50**.
* **Eligibility:** Verified **email/phone**, **DL/State ID** (pre‑publish), **SSN last‑4** (individual) or **EIN** (org), **US bank account**.
* **Reserves:** risk‑based, default **0–20%** for **30–60 days** (configurable).
* **Platform:** **Stripe** (cards, Apple/Google Pay).

## 24.0 Architecture choice (Stripe model)

**MVP approach:** **Stripe Connect Express + Separate Charges and Transfers (SCaT)**

* **Charges** happen on the **platform account** (our Stripe), so checkout is unified.
* **Funds** are held in our ledger until payout; at payout, we create a **Transfer** to the organizer’s **Connected Account** (Express).
* Stripe then **auto‑pays out** from the connected account to the organizer’s bank per Stripe’s payout schedule (daily/weekly; Express default is **automatic**, next available, which satisfies our “payout on campaign end” promise once we transfer).
* We can **hold reserves** by **under‑transferring** and releasing later via a second transfer.
* **KYC/KYB & bank**: handled via Stripe Express onboarding (we still show our Verification page with status mirroring).
* **1099‑K/KYB tax**: Stripe handles for Express (future‑proof).

Alternative (deferred): Platform‑managed payouts to external bank accounts without Connect. **We are not using this** at MVP for compliance and speed.

## 24.1 Key entities & data model (extends §8)

**Organizer (entity)**

* stripe\_connected\_account\_id (required for payout)
* kyc\_status ('unverified'|'pending'|'verified'|'rejected'|'hold')
* bank\_status ('unlinked'|'pending'|'verified'|'returned')

**Campaign**

* status ('draft'|'live'|'ended'|'not\_funded'|'suspended')
* end\_date, payout\_eligibility\_at = end\_date + hold\_days (business‑day aware)
* payout\_policy\_snapshot (goal model, reserves %, min payout)

**Finance objects**

finance.wallet

- organizer\_id, available\_cents, on\_hold\_cents, reserved\_cents, negative\_cents

finance.payout

- id, organizer\_id, campaign\_id, connected\_account\_id,

amount\_gross\_cents, reserve\_cents, net\_transfer\_cents,

stripe\_transfer\_id, stripe\_transfer\_status ('none'|'pending'|'paid'|'failed'|'canceled'),

stripe\_payout\_id, stripe\_payout\_status ('none'|'in\_transit'|'paid'|'failed'|'canceled'),

due\_at, requested\_at, approved\_at, processing\_started\_at, paid\_at, returned\_at,

return\_code?, review\_reason?, dual\_approval\_required bool, approved\_by?, second\_approved\_by?,

statement\_url?, audit\_jsonb, created\_at, updated\_at

finance.payout\_item

- payout\_id, donation\_id, amount\_cents (immutable snapshot)

finance.reserve\_release

- id, organizer\_id, campaign\_id, release\_at, amount\_cents, status ('scheduled'|'transferred'|'canceled'), transfer\_id?

finance.ledger (double‑entry appendix)

- id, ts, entry\_type ('donation','refund','chargeback','transfer','reserve','release','adjustment'),

debit\_account, credit\_account, amount\_cents, ref\_ids {}

**Donation** (add fields)

* transfer\_group (campaign scoped), included\_in\_payout\_id?, aon\_auto\_refunded bool

## 24.2 Eligibility gates (pre‑payout checklist)

A campaign becomes **payout‑eligible** when all green:

1. **Campaign state:** ended and not suspended; (AoN: must be **funded**).
2. **Hold window:** end + **3–5 business days** (admin config, default 3).
3. **Identity:** Organizer verified **email/phone + DL/State ID** (pre‑publish), **SSN last‑4** (individual) or **EIN** (org).
4. **Bank:** US bank account **verified** on the connected account.
5. **Minimum balance:** **≥ $50** available (after refunds/chargebacks to date).
6. **Risk/Compliance:** No active **compliance hold** (Section 5 triggers).
7. **No negative balance** that would over‑offset the payout (if exists, net out first).

**AC‑ELIG‑1:** Wallet “Payout” button shown only when all above are true; otherwise a checklist shows blocking items with CTAs.

## 24.3 Accrual & balance math (recap from §2)

For each **succeeded** donation:

* Compute **Net to campaign (N)** using the chosen cover‑fees model; log in **ledger**.
* Wallet: available += N (if before campaign end → logically on campaign balance that will be eligible later).
* On **refund/chargeback**: reverse entries; if post‑payout → **negative balance** increases.

**Organizer wallet presentation (UI):**

* **Available** (eligible now)
* **On hold** (hold window)
* **Reserved** (risk reserve)
* **Negative** (owed due to post‑payout refunds/chargebacks)

## 24.4 Scheduler & batch creation

**Nightly job** + **real‑time triggers** check campaigns that **ended** and passed **hold window**.

**Steps:**

1. Pull campaigns with status=ended and payout\_eligibility\_at ≤ now and not yet paid.
2. Compute **eligible amount** = campaign\_net − prior\_payouts − refunds\_to\_date − reserves\_to\_hold − negative\_offset.
3. If eligible\_amount ≥ $50 → propose **Payout batch**.
4. **Dual‑approval** if eligible\_amount ≥ threshold (default **$50,000**) or if **risk flag** present.
5. Create **finance.payout** (state = requested if Organizer pressed button; else due → processing\_started by scheduler).
6. Snapshot donation rows into **payout\_item** (immutable).
7. Move amount from **available → on\_hold** while processing to avoid double spend.

**Idempotency:** Use (campaign\_id, run\_date) as **composite idempotency key**; re‑runs should no‑op if payout exists.

## 24.5 Execution with Stripe (SCaT)

**Goal:** Transfer net\_transfer\_cents to the organizer’s **connected account**; Stripe then pays out to bank.

**Transfer creation**

* transfer = stripe.transfers.create({ amount, currency:'usd', destination: connected\_account\_id, transfer\_group })
* transfer\_group = 'campaign:{shortId}' to link all transfers for that campaign.
* Store stripe\_transfer\_id, set stripe\_transfer\_status='pending'.

**On success:**

* Update status → paid.
* Wallet: on\_hold -= amount; (if you moved it on hold)
* Stripe **payout** will occur per connected account schedule. We **listen** for webhooks:
  + payout.created, payout.paid, payout.failed, payout.canceled **on the connected account** (requires Connect events forwarding).
  + Link payout to this transfer by inspecting **balance transactions** or transfer.destination\_payment relations.

**On failure:**

* Mark stripe\_transfer\_status='failed' and retry (see 24.6).
* Keep funds on\_hold until resolved.

**Reserves:**

* If reserve\_cents > 0, we **under‑transfer** (amount = eligible − reserve).
* Create **finance.reserve\_release** scheduled for release\_at (30–60 days).

## 24.6 Retries & error handling

**Transfer errors** (API/network):

* Retries with exponential backoff, max 5 attempts; idempotency key payout:{id}.
* On persistent failure: state → in\_review; Finance Ops alerted; user sees banner.

**Payout failures/returns** (bank issues on connected account):

* Webhook payout.failed or payout.canceled with **return\_code** (e.g., account\_closed, no\_account).
* Set stripe\_payout\_status='failed'; mark payout **Returned**.
* **Notify organizer** per §18 (SMS → **Voice fallback**, Email, In‑app).
* Wallet wise: Stripe returns funds to connected account balance; **we** must **reverse the original transfer** or create a **negative transfer** back to platform balance depending on Stripe behavior/config.
  + **Default (simpler):** Do **not** auto‑reverse. Ask organizer to **update bank**; Stripe will **auto‑retry** payout on next cycle.
  + **If platform must hold** (risk): Finance can **reverse transfer** (admin tool) → funds appear in platform balance; payout marked **Returned (platform hold)**.

**Resubmit flow (after bank update)**

* Finance or scheduler triggers **transfer re‑attempt** if we reversed; or simply waits for **Stripe auto‑payout** if we left transfer on connected account.

**AC‑RET‑1:** Returned payouts trigger organizer alerts and Support case creation (23.0) if unresolved after 7 days.

## 24.7 Reserves (risk‑based)

* **Policy knobs (Admin → Finance)** (§20.I):
  + Default: Low risk **0%**, Elevated **10%/30 days**, High **20%/60 days**.
  + Assignment: **Risk Analyst** can set per organizer or per campaign.
* **Accounting:** At payout creation, compute reserve\_cents and **withhold** by under‑transferring.
* **Release job**: daily checks **reserve\_release** rows with release\_at ≤ now and organizer not suspended; creates **new transfer** to connected account for amount\_cents.
* **Display:** Wallet shows **Reserved** and next **release date**; Organizer gets **release confirmation** when transferred.

**AC‑RES‑1:** Releasing reserves auto‑notifies organizer; ledger entries keep clear chain.

## 24.8 Post‑payout refunds, disputes & negative balances

* **Refund after payout:**
  + Wallet becomes **negative** by the refunded net amount.
  + Future payouts **offset** negative first (organizer sees banner “Negative balance will be recovered from future funds”).
* **Chargeback lost:** deduct disputed amount + fee → negative.
* **No future funds:** escalate to **collections** workflow (Admin case; configurable dunning emails).

**AC‑NEG‑1:** Organizers cannot **withdraw** until negative = 0; payouts blocked across **all campaigns** linked to that organizer.

## 24.9 Statements & exports

**Organizer-facing statements (per payout)**

* **Header:** Payout ID, Campaign, Date ranges, Connected Account last‑4, Status.
* **Summary:** Gross donations in period, refunds/chargebacks, fees (memo), reserve held/released, net transferred, payout status.
* **Itemization:** donations included (id, date, donor privacy mode, amount).
* **CSV export**: donations & summary.

**Admin finance reports (daily)**

* Payouts created/paid/returned, reserves scheduled/released, negative balance changes, deltas per organizer.

**AC‑STM‑1:** Statement totals reconcile to ledger entries (24.12).

## 24.10 Roles, approvals & admin tools (ties to §20.D)

**Approvals**

* **Auto‑approve** under threshold and no risk flags.
* **Dual approval** (two distinct Finance roles) when:
  + Amount ≥ **$50,000** or
  + Organizer risk level **High** or
  + Manual override requested.

**Admin actions**

* View payout queue (Due, In review, Processing, Returned).
* Approve/Reject/Cancel before transfer; **Reverse transfer** (if allowed) after return.
* Adjust reserve % and release date; trigger early release with reason.
* Edit connected account metadata (read‑only bank details; initiate “Update bank” email).
* Simulate payout math “What‑if” (like §2.10 simulator for donations).

**Audit**

* Every approval, reversal, reserve change logged to admin.audit\_log with reason code.

## 24.11 Notifications map (tie to §18)

* **Payout ready** → Organizer (Email + In‑app): “Payout available after {date}.”
* **Payout initiated** → Organizer: “We started your payout for {campaign}.”
* **Payout paid** → Organizer: “Payout paid. Statement inside.”
* **Payout returned (critical)** → **SMS → Voice fallback** + Email + In‑app.
* **Reserve release** → Organizer (Email + In‑app).
* **Compliance hold** → Organizer (Email + In‑app) with reason and next steps.

## 24.12 Ledger (double‑entry mapping)

(High level—implementation can use accounting subledgers, but invariants must hold.)

**Accounts**

* Donations:Campaign:{id} (liability)
* Reserves:Campaign:{id} (liability)
* Organizer:Wallet:{organizer\_id} (liability)
* Cash:Platform (asset)
* Cash:Stripe Connected:{acct} (asset memo) — optional tracking
* Fees (memo) — reports only

**Events**

* **Donation succeeded:**
  + DR Cash:Platform / CR Donations:Campaign (amount N)
  + DR Donations:Campaign / CR Organizer:Wallet (N) (internal move when confirming net)
* **Refund (pre‑payout):** reverse above proportionally.
* **Payout transfer:**
  + DR Organizer:Wallet / CR Cash:Platform (transfer amount)
  + (Optionally track memo move to *Cash:Stripe Connected*)
* **Reserve held:**
  + DR Organizer:Wallet / CR Reserves:Campaign (amount)
* **Reserve release:**
  + DR Reserves:Campaign / CR Organizer:Wallet
  + Then standard **payout transfer** for released amount.
* **Negative balance offset:** future **DR Wallet** reductions before transfer.

**Invariant:**  
Wallet.available + Wallet.on\_hold + Wallet.reserved - Wallet.negative = Sum(N donations) - Sum(transfers out) - Sum(refunds/chargebacks)

## 24.13 Wireframe callouts (Organizer & Admin)

### Organizer — ****Wallet > Payouts**** (portal)

1. **Summary bar:** Available / On hold / Reserved / Negative (with info tooltips).
2. **Eligibility checklist** card (ticks with CTAs): ID verified, SSN/EIN verified, Bank verified, Hold ends on {date}, Balance ≥ $50.
3. **Payout card (if eligible):**
   * Amount to transfer now, Reserve to hold, Next reserve release date.
   * **Request payout** button (if manual trigger enabled) or **“Scheduled for {date}”** label (auto).
4. **History table:** Date, Campaign, Amount, Reserve, Status (Processing/In transit/Paid/Returned), Statement link.
5. **Returned banner** (if any): “We couldn’t deliver your payout — update your bank.” → **Update bank** CTA (Stripe hosted).
6. **Education box:** “How payouts work” (KB links).

### Admin — ****Finance Ops > Payouts queue****

1. Filters: Status, Risk level, Amount range, Organizer.
2. **Row:** Organizer → Campaign → Amount → Reserve → Due at → Risk badge → **Actions** (Approve, Hold, Reverse [if returned], Statement).
3. **Detail drawer:** ledger snapshot, donation list, webhooks timeline, connected account health, prior returns.

## 24.14 Risk & compliance hooks (Section 5)

* **Risk elevates holds/reserves** and can **delay transfer** (state = in\_review).
* **Triggers**: high dispute rate, velocity anomalies, OFAC watchlist hits via Stripe, mismatched names, repeated returned payouts.
* **Outcomes**: increase reserve %, extend release date, require additional verification, or suspend payouts.

## 24.15 Instrumentation & metrics

**Events**

* payout\_due{campaign\_id, amount, reserve}
* payout\_request{by} / payout\_approve{dual} / payout\_transfer\_success|fail
* payout\_payout\_paid|failed{return\_code}
* reserve\_set{percent, days} / reserve\_release
* wallet\_negative\_change{delta}

**Dashboards**

* Time to pay (end → paid), % payouts paid < 5 business days, return rate, reserve outstanding, negative balance exposure, top organizers by payout volume, webhook latency.

**Alerts**

* Return rate spike (>2% weekly), webhook delays, transfer API failures >1%, payouts stuck processing > 24h, reserve releases overdue.

## 24.16 Acceptance Criteria (summary)

1. **Eligibility** correctly gates payouts; UI checklist with CTAs is accurate.
2. **Scheduler** creates payout batches at end+hold; idempotent; snapshots donations.
3. **Stripe execution**: transfers created with idempotency; statuses flow to **Paid**; connected payouts reflected in our UI via webhooks.
4. **Returns** trigger organizer alerts (SMS→Voice fallback + Email + In‑app); Admin queue shows return code and next steps.
5. **Reserves** withheld and later released via separate transfers; organizer sees dates/amounts.
6. **Refunds/chargebacks** post‑payout create negative balances and block future payouts until cleared.
7. **Statements** downloadable; totals match ledger; payout history shows accurate statuses.
8. **Approvals** enforce dual‑approval thresholds; all admin actions audited.
9. **Security & privacy**: bank details never shown in full; use Stripe hosted flows; PII protected.
10. **Monitoring** and alerts live; SLO: 99% payouts paid within **5 business days** of end+hold, excluding organizer‑caused delays.

## 24.17 QA plan (tie to §22)

* Create campaigns with various outcomes: KWR ended; AoN funded; AoN not funded (no payout).
* Verify eligibility checklist blocks until ID/SSN/Bank complete.
* End campaign; simulate hold passing (clock travel) → scheduler creates payout; confirm donation snapshot.
* Stripe transfer success → webhook → status paid → payout history updates; statement totals reconcile.
* Force payout.failed on connected account → **Returned** flow; alerts via SMS→voice; “Update bank” CTA → resubmit → paid.
* Reserve 10%/30d set → under‑transfer; after 30d, release transfer fires; organizer notified.
* Post‑payout refund → negative balance; next campaign payout offsets negative first; UI banners accurate.
* Dual‑approval path for ≥ $50k — require two approvers; audit shows both.
* Idempotency: retry transfer call; confirm single payout.
* Analytics events visible; alerts configured.

## 24.18 Roadmap (Phase‑2/3)

* **Same‑day or Instant Payouts** (Stripe Instant Payouts) for low‑risk organizers (fee trade‑off).
* **ACH / Bank‑to‑bank donations** (lower fees) with delayed availability rules.
* **Organizer wallet interest (sweep)** via Stripe Treasury (longer‑term).
* **Multi‑campaign consolidation payouts** (organizer chooses monthly).
* **Per‑campaign fee sponsorship** (org pays donor fees) with per‑payout adjustments.
* **Automated reserve tuning** via risk scores.