Instrumentation plan

A pragmatic event taxonomy + funnel plan to measure outcomes, protect trust, and support experimentation.

Instrument the experience so you can prove impact, diagnose issues, and run trustworthy experiments—without drowning in events.

Event taxonomy and naming

Naming convention: **object_action** (e.g., rec_module_viewed, rec_item_clicked). Use consistent nouns and past-tense actions.

Event name	When it fires	Required properties
rec_module_viewed	Recommendation module enters viewport	user_id, session_id, surface, experiment_id, variant_id, position
rec_item_impression	A recommended item is rendered	item_id, item_type, rank, model_version, rationale_code
rec_item_clicked	User clicks a recommended item	item_id, rank, surface, experiment_id, variant_id
rec_item_dismissed	User dismisses / hides an item	item_id, reason (optional), rank, model_version
content_consumed	Content is completed / meaningful dwell	content_id, format, duration, completion_pct
tool_started	User starts a high-value tool	tool_id, entry_point, experiment_id, variant_id
tool_completed	User completes the tool	tool_id, completion_time, success_flag
feedback_submitted	Explicit feedback is given	type, sentiment, free_text (optional), surface

Funnels and KPIs

Funnel	Definition	Primary KPI
Discovery to action	rec_module_viewed -> rec_item_clicked -> tool_started	CTR, tool start rate
Action to completion	tool_started -> tool_completed	Completion rate, time-to-complete
Engagement quality	content_consumed (>=X sec) + repeat visits	Qualified engagement rate
Trust health	dismissals + negative feedback + support contacts	Dismiss rate, complaint rate

Data quality checklist

- Events fire once per exposure (no duplicates) and include experiment identifiers.

- Exposure is logged (who saw what) for valid attribution.

- Timestamps are consistent (server vs client) and timezone-safe.

- Properties are typed and validated (IDs, enums, null behavior).

- Dashboards match source-of-truth queries (no "Excel math").

Privacy and retention notes

- No sensitive attributes stored in event payloads unless explicitly approved.

- PII is minimized; IDs are hashed/tokenized where appropriate.

- Retention policy documented; access controlled and auditable.