

06 · Environment variables & secrets

Verified live 2026-06-30. Every environment variable the website reads, what it does, and how sensitive it is for the test→live switch. Cross-refs: integrations 04-integrations.md, go-live 07-go-live-checklist.md, audit AUDIT-FINDINGS.md. **Sensitivity** = how much care the test/live transition needs: LIVE-critical (wrong value = real money or broken prod), changes behavior, low.

Stripe

Var	Purpose	Sensitivity
STRIPE_SECRET_KEY	Stripe API key. <code>sk_test...</code> prefix toggles test mode (inline products); live key → hardcoded live Product IDs	LIVE-critical — swap starts real charges
STRIPE_WEBHOOK_SECRET	Verifies <code>api/stripe-webhook.js</code> signatures	must match the live endpoint
STRIPE_CONNECT_WEBHOOK_SECRET	Verifies <code>api/stripe-connect-webhook.js</code> (separate endpoint)	must match the live Connect endpoint
FRIEND_COUPON_DIGITAL / _EXPERT / _CONCIERGE	Live friend-discount coupon ids per tier (B2T1aavc / ArPaJugz / B1sqQ2mS)	
FRIEND_COUPON_DIGITAL_TEST / _EXPERT_TEST / _CONCIERGE_TEST	Sandbox coupon ids used in test mode	test-only

Changing the friend-discount coupons (no code change needed): these env vars are currently **unset** — the code falls back to the hardcoded ids above (`api/create-checkout-session.js` ~line 44). To switch to a different coupon: create the new coupon in Stripe (any duration — "once"/"forever" is irrelevant for one-time payments; just don't set a redemption limit), then set the matching `FRIEND_COUPON_*` env var in Vercel to the new coupon **ID** and redeploy. The env var wins over the hardcoded fallback. Never delete a coupon that is still referenced (env value, or the fallback when the env is unset) — referred-friend checkouts would start failing to apply the discount.

URLs

Var	Purpose	Sensitivity
URL	Base site URL	
PUBLIC_BASE_URL / VERCEL_URL	Public base for building links/redirects	

Email (Resend)

Var	Purpose	Sensitivity
RESEND_API_KEY	Resend auth. Missing → email skipped (logged, not thrown)	
RESEND_FROM_EMAIL	Sender. Default <code>onboarding@resend.dev</code> is the Resend sandbox — change to a verified <code>@nieexpertsspain.com</code> sender at go-live (B1)	
EMAIL_OVERRIDE_TO	Redirects all mail to one test inbox (subject [TEST-...]). UNSET at go-live (B2)	— leaving it set means no customer gets mail
EMAIL_DELAY_MINUTES	Send delay (order confirmation default 5, welcome 0, magic-link never)	
EMAIL_HEADER_STYLE	Branded header style toggle	

Notion

Var	Purpose	Sensitivity
NOTION_API_KEY	Notion integration token	
NOTION_DATABASE_ID	"NIE Website Orders" DB id	

n8n bridge

Var	Purpose	Sensitivity
N8N_W01_WEBHOOK_URL	Order creation / Fase-1 invite bridge	
N8N_W01B_WEBHOOK_URL	Companion W01b bridge	
N8N_W08_WEBHOOK_URL	Abandoned-checkout (checkout.session.expired)	
N8N_W09_WEBHOOK_URL	Upsell handler	
N8N_W10_WEBHOOK_URL	Chargeback / dispute	
N8N_W16_WEBHOOK_URL	Refund handler	
N8N_BRIDGE_SECRET	Shared secret authenticating website→n8n bridge calls	shared secret — rotate if exposed

Discord

Var	Purpose	Sensitivity
DISCORD_WEBHOOK_URL	#stripe-checkouts (also upsell embeds)	
DISCORD_AFFILIATE_WEBHOOK_URL	#affiliation	
DISCORD_PAYOUT_WEBHOOK_URL	#affiliation-payout	

Supabase

Var	Purpose	Sensitivity
SUPABASE_URL	Project URL (kbmvtawsdhmzjnsonazr)	
SUPABASE_SERVICE_ROLE_KEY	Service-role key — bypasses RLS ; the entire security posture rests on it never leaking	highly sensitive

Affiliate payout

Var	Purpose	Sensitivity
CRON_SECRET	Authorizes payout cron endpoints (payout-notify, payout-approve). Fail-closed	payout-critical
PAYOUT_DRY_RUN	=1 is an absolute no-money brake (no transfers execute). Leave =1 until really paying	money brake
AFFILIATE_HOLD_DAYS	Days a commission is held before payable (default 30)	
AFFILIATE_PAYOUT_MIN_EUR	Minimum payout threshold (default €1 — no threshold, Christian 2026-07-03)	
AFFILIATE_AUTH_SECRET	HMAC secret for magic-link / session / payout tokens. Throws if unset	
AFFILIATE_ADMIN_TOKEN	Admin auth for affiliate admin actions	
AFFILIATE_DASHBOARD_URL	Base URL for the affiliate dashboard links	

Security / captcha

Var	Purpose	Sensitivity
TURNSTILE_SECRET_KEY	Cloudflare Turnstile for signup captcha. Unset = dev passthrough (no captcha); set = fail-closed . Prod must set (B5)	

Secrets handling

- Secrets live in **Vercel env** (website) and **macOS Keychain** (local), referenced by name only — **never committed** to the repo.
- **Rotate any secret shared during setup** — including Stripe test keys, Supabase PAT, Notion, Resend, and Tally keys pasted in chat — before or at go-live.
- The **n8n instance holds its own credentials internally** : Postgres (Supabase service), Resend, Google Drive, and Discord. These are separate from the website's env and are part of the handed-over tooling — rotate them on the same go-live pass.
- Service-role and HMAC secrets (`SUPABASE_SERVICE_ROLE_KEY`, `AFFILIATE_AUTH_SECRET`, `N8N_BRIDGE_SECRET`, `CRON_SECRET`) are the crown jewels: a leak of any one weakens a whole subsystem. See AUDIT-FINDINGS **H1** for the RLS-zero-policies posture that makes the Supabase key especially load-bearing.