VELTRIS GROUP LTD

PLAYBOOK · ENGINEERING

The 47-point pre-launch checklist

Every check we run the week before a Next.js site goes live — performance, security, SEO, accessibility, observability, rollback posture, content, and legal surfaces.

Author: Maria Georgiou · Head of Engineering · VELTRIS GROUP LTD

How to use this edition

Veltris runs this gate the week before a Next.js property is allowed to ship to production. It is written for engineers, but security, SEO, accessibility, observability, content, and legal checks are included because launches fail at interfaces, not in the framework release notes.

Each item is a binary pass/fail for that moment in time. A “fail” does not always block launch—it must have a named risk owner, compensating control, and dated remediation in the runbook you attach to the release ticket.

Numbers reference the canonical web edition at veltris.info/playbooks/pre-launch-checklist so annotations stay in sync when we revise the list.

#1 · Performance

Pass when: Largest Contentful Paint (LCP) meets budget on critical templates

Why: LCP is the strongest lab proxy for perceived load on marketing and app shells; regressions here show up as bounce before analytics fires.

Verify: Run Lighthouse (mobile, throttled) on `/`, top money URL, and logged-in shell; confirm LCP d internal budget (commonly 2.5–4.0s lab). Cross-check `next dev` never used for numbers.

#2 · Performance

Pass when: Cumulative Layout Shift (CLS) is controlled for fonts, ads, and late images

Why: CLS erodes trust on checkout and forms; most spikes come from webfonts swapping and unsized media.

Verify: In Performance panel, throttle CPU 4× and reload; watch Layout Shifts panel. Confirm `next/image` width/height (or fill + aspect), `font-display: swap` with reserved space, and no third-party banners injecting above static height.

#3 · Performance

Pass when: JavaScript bundles for first navigation are right-sized and split

Why: Hydration cost dominates TTI on React sites; accidental barrel imports inflate server components boundaries.

Verify: Compare `.next/static/chunks` after `pnpm build`; spot-check largest entry with `npx @next/bundle-analyzer` or source-map-explorer. Grep for `import *` from icon/UI libraries and remove.

#4 · Performance

Pass when: Images use modern formats and sane breakpoints for hero and grids

Why: Oversized JPEG/PNG is still the default failure mode on hand-authored content.

Verify: Network tab: confirm `content-type` prefers AVIF/WebP where configured. Spot-check `sizes` attribute matches layout at md/lg breakpoints.

#5 · Performance

Pass when: Server components / data fetching avoid waterfalls on above-the-fold

Why: Serial `await` in nested layouts stacks latency in a way Lighthouse may under-report vs real geography.

Verify: Trace server logs or Vercel function timeline; parallelize independent fetches with `Promise.all`. Confirm no accidental `fetch` per row in lists without batching.

#6 · Performance

Pass when: Edge and CDN caching policies match content freshness class

Why: Stale HTML with fresh JSON confuses SEO and auth; aggressive `s-maxage` on personalized routes breaks GDPR expectations.

Verify: curl `-I` on static, ISR, and authenticated routes; map `cache-control`, `cdn-cache-control`, and `set-cookie` interactions. Document TTL table in runbook.

#7 · Performance

Pass when: Prefetch and `loading="lazy"` defaults do not starve critical imagery

Why: Over-prefetching competes with LCP image on constrained networks.

Verify: Disable network cache, reload, and confirm LCP element begins download before low-priority images. Audit `<Link prefetch>` density on mega-navs.

#8 · Security

Pass when: No server secrets or private keys ship to the client bundle

Why: Accidental `NEXT_PUBLIC_` prefixes and copied `.env` lines are the fastest path to credential rotation at launch.

Verify: Run `pnpm build` then `grep -R "sk_" .next` (Stripe) and `grep -R "BEGIN PRIVATE" .next` expecting zero hits. Spot-check `process.env` usage in shared modules.

#9 · Security

Pass when: Security headers present: HSTS, X-Frame-Options, nosniff, Referrer-Policy baseline

Why: Headers are cheap insurance against clickjacking, MIME sniffing, and SSL strip on first visit.

Verify: `curl -sI https://<prod-host>/` and compare to internal baseline (often aligned with OWASP cheat sheet). Confirm HSTS max-age only after HTTPS verified end-to-end.

#10 · Security

Pass when: Content-Security-Policy is enforced or staged in report-only with monitored reports

Why: CSP is the main guardrail against XSS exfiltration when HTML escapes fail.

Verify: Search `next.config` middleware or edge for `Content-Security-Policy`. If report-only, open reporting endpoint dashboard for spikes the week pre-launch.

#11 · Security

Pass when: Authentication cookies are HttpOnly, Secure, SameSite-appropriate

Why: Session fixation and CSRF surface area explodes when cookies are readable from JS.

Verify: Inspect `Set-Cookie` in Network after login; confirm flags. For cross-site flows, validate OAuth state + PKCE parameters against provider docs.

#12 · Security

Pass when: Dependency and container image scan is clean at agreed severities

Why: Launch traffic attracts opportunistic scanning; known RCEs in transitive deps become incidents.

Verify: `pnpm audit --prod` or GitHub Dependabot export; triage critical/high with owners. Record accepted risks with compensating controls.

#13 · Security

Pass when: Rate limiting and bot protection exist on auth, contact, and webhook routes

Why: Credential stuffing and webhook replay spike at public launch.

Verify: Hit `/api` routes with scripted bursts in staging; confirm 429 and backoff headers. Validate webhook signatures with rotated secrets per env.

#14 · Security

Pass when: CORS and `Access-Control-Allow-Origin` are not wildcarded with credentials

Why: Misconfigured CORS leaks session-backed JSON to arbitrary origins.

Verify: Read API middleware CORS builder; test preflight from a disallowed origin in browser devtools. Confirm `credentials: true` pairs with explicit allowlist.

#15 · SEO

Pass when: `robots.txt` allows indexing intent and blocks private surfaces

Why: Staging leakage and accidental `Disallow: /` are classic launch-week fires.

Verify: Fetch `/robots.txt` in prod; confirm sitemap URL, no broad disallow on public templates, and disallow on `/api`, drafts, and internal tools.

#16 · SEO

Pass when: XML sitemap lists only 200 URLs with canonical content

Why: Sitemaps are a crawl budget signal; polluted feeds slow discovery of money pages.

Verify: Parse `/sitemap.xml` (or index); sample 20 URLs with `curl -o /dev/null -s -w "%{http_code}"` expecting 200. Remove parameterized duplicates already canonicalized.

#17 · SEO

Pass when: Canonical tags resolve duplicate hosts, trailing slashes, and UTM variants

Why: Split signals dilute rankings and confuse attribution.

Verify: View-source on parameterized marketing URLs; confirm `<link rel="canonical">` points to preferred absolute URL. Test `www` vs apex redirect policy once.

#18 · SEO

Pass when: Structured data validates for templates that earn rich results

Why: Invalid JSON-LD can suppress enhancements and flag Search Console issues on day one.

Verify: Run Google Rich Results Test on Article/Product/FAQ templates; fix required fields. Keep `@id` stable across ISR regenerations.

#19 · SEO

Pass when: Meta titles and descriptions are unique per indexable route

Why: Duplicate titles cap CTR and make Search Console noise unreadable.

Verify: Export routes from sitemap; script `curl` + `grep -o "<title>[^<]*"` uniqueness check. Manual spot-check for dynamic `[slug]` fallbacks.

#20 · SEO

Pass when: Hreflang (if multi-locale) is reciprocal and uses x-default

Why: Broken reciprocity causes hreflang clusters to be ignored entirely.

Verify: Pick two locales; each page lists the other with matching pairs; `x-default` points to global fallback. Verify no 404s in hreflang set.

#21 · SEO

Pass when: Redirect chains are shallow and preserve method where needed

Why: Deep chains burn crawl budget and drop referral headers on POST upgrades.

Verify: Run Screaming Frog or `curl -IL` on top 50 legacy URLs from migration sheet; d2 hops, no 302’301 mixes on permanent moves.

#22 · Accessibility

Pass when: Text and interactive contrast meet WCAG AA for default theme

Why: Brand blues on white often fail 4.5:1 for body copy when designers optimize for aesthetics only.

Verify: Axe DevTools contrast rules on light/dark; spot-check primary buttons and error text. Log exceptions only where documented design debt exists.

#23 · Accessibility

Pass when: Full keyboard navigation covers modals, menus, and cookie banners

Why: Trapped focus in overlays is a lawsuit-shaped bug on marketing sites.

Verify: Tab through header nav, mobile drawer, cookie CMP, and checkout modals; confirm Esc closes, focus returns to trigger, and no positive tabindex hacks.

#24 · Accessibility

Pass when: Visible focus states are not removed by global CSS resets

Why: `outline-none` without replacement hides keyboard users entirely.

Verify: Search global CSS for `outline: none`; ensure paired `:focus-visible` ring utilities. Visual check Tab path on long forms.

#25 · Accessibility

Pass when: Images have accurate `alt`; decorative images use empty alt

Why: Screen readers announce filename garbage when `alt` is missing or stuffed with keywords.

Verify: Axe "image-alt" pass on top templates; CMS training snippet reviewed. Hero alt describes destination, not "image of laptop".

#26 · Accessibility

Pass when: Form errors associate programmatically with fields (`aria-describedby` / `role=alert`)

Why: Color-only error states fail WCAG and frustrate conversions.

Verify: Submit empty checkout/contact; VoiceOver or NVDA announces error text tied to inputs. Server errors map to field-level messages.

#27 · Accessibility

Pass when: Heading hierarchy is logical (single h1, no skipped levels for layout)

Why: Heading order is the primary navigation model for many AT users.

Verify: HeadingsMap extension or axe "heading-order"; fix card grids that misuse `h3` without parent `h2`.

#28 · Accessibility

Pass when: Skip link targets main content and works across client navigations

Why: SPA re-renders can drop focus management on route change.

Verify: Keyboard-only: activate skip link on home, navigate to inner page, confirm skip link still first tab stop and `#main` exists.

#29 · Observability

Pass when: Error boundaries capture client exceptions without silent failures

Why: White screens without tickets are worse than noisy alerts pre-launch.

Verify: Trigger known error in staging with `throw`; confirm boundary UI and Sentry/Browser SDK event with release tag and route.

#30 · Observability

Pass when: Server logs exclude PII and secrets at default log levels

Why: Log drains become compliance incidents when bodies include emails or tokens.

Verify: Sample staging logs for `authorization`, `cookie`, `email` substrings; scrub serializers. Confirm `NEXT_RUNTIME` log redaction middleware active.

#31 · Observability

Pass when: Synthetic uptime checks hit auth-free health endpoints

Why: Checking `/` alone misses API brownouts that users feel in AJAX flows.

Verify: Configure Pingdom/Better Stack against `/api/health` (DB ping) and edge region matrix; alert thresholds documented in runbook.

#32 · Observability

Pass when: Metrics and traces correlate user session with deployment version

Why: Without release tags, post-launch regressions are archaeology.

Verify: Open one trace in APM; confirm `service.version` or `VERCEL_GIT_COMMIT_SHA` attribute. Validate sampling not starving error spans.

#33 · Observability

Pass when: Alert routes are owned (PagerDuty/Opsgenie) and not a shared inbox black hole

Why: Launch week noise causes mute-all, which hides the first real outage.

Verify: Table-top one synthetic failure; confirm on-call ack SLA. Mute rules documented with expiry.

#34 · Observability

Pass when: Background jobs / queues expose depth metrics and dead-letter handling

Why: Email and webhook workers backlog silently until SLA breach.

Verify: Dashboards for queue depth, age-of-oldest-job, DLQ rate; run load test that enqueues burst; verify autoscale or backpressure behavior.

#35 · Content

Pass when: Legal, privacy, cookies, and imprint pages reflect shipping jurisdictions

Why: Placeholder Latin text in footer links is an embarrassing and sometimes binding compliance gap.

Verify: Human read diff vs last approved legal copy; confirm entity name, address, VAT, DPO/contact email, and last-updated date match footer cross-links.

#36 · Content

Pass when: Pricing and fee copy include required disclaimers for regions you ship

Why: Marketing promises without qualifiers create chargeback and ASA/FTC exposure.

Verify: Legal checklist mapped per country; footnotes present on promotional modules. Currency formatting uses explicit ISO codes where multi-currency.

#37 · Content

Pass when: 404 and 500 pages are branded, accessible, and log correlation IDs

Why: Default Next errors leak stack vibes and lose support signal.

Verify: Hit unknown route and forced error route; screen reader announces heading; support ID visible matches log field.

#38 · Content

Pass when: Open Graph and Twitter cards resolve on first share for launch URLs

Why: First investor tweet with broken `og:image` is permanent screenshot embarrassment.

Verify: Facebook Sharing Debugger + Twitter Card Validator on `/`, article template, and product template after cache purge.

#39 · Content

Pass when: Contact and demo forms have spam controls (honeypot, Turnstile, or rate limit)

Why: Public forms become DDoS via email gateways within hours of launch posts.

Verify: Submit from automation without browser token expecting block; confirm deliverability path still works for legitimate Gmail.

#40 · Content

Pass when: i18n strings have no missing keys in default locale on critical flows

Why: Missing translation keys surface as raw IDs in production builds.

Verify: Run i18n extraction/compile step if used; click through checkout/account in default language with pseudo-localization off.

#41 · Legal

Pass when: Cookie consent blocks non-essential scripts until affirmative action (EEA/UK)

Why: Pre-ticking or implied consent violates ePrivacy interpretations enforced in CY/EU clients.

Verify: Clear site data, reload, network tab shows marketing pixels absent until accept. Record CMP vendor configuration export.

#42 · Legal

Pass when: Privacy policy lists processors (analytics, email, hosting) with DPA status

Why: GDPR accountability expects Article 30 records to match public disclosures.

Verify: Table match between subprocessors page and DPAs on file; owner names and data categories accurate for actual integrations enabled in prod.

#43 · Legal

Pass when: Terms of service version is bumped if liability, payment, or SLA clauses changed

Why: Silent edits destroy enforceability if dispute arises post-launch.

Verify: Legal diff reviewed; `Last updated` ISO date set; major change comms drafted if B2C consumer rights affected.

#44 · Legal

Pass when: Export control / sanctions disclaimers present if dual-use software is described

Why: Deep technical playbooks can trigger compliance review when audiences are global.

Verify: Legal classification questionnaire completed; site copy includes required cautionary language or geo-gating decision documented.

#45 · Legal

Pass when: Accessibility statement published where law mandates (public sector) or voluntarily

Why: Some RFPs require WCAG conformance claim with feedback channel.

Verify: Link in footer works; states standard (2.1 AA), known exceptions, and contact path for issues.

#46 · Legal

Pass when: Marketing claims in hero metrics are substantiated with methodology footnotes

Why: ASA/SEC-style scrutiny applies to some Veltris clients; vague multiples invite legal review.

Verify: Each hero stat has citation URL or internal doc ID in CMS footnote field; finance signed off where revenue claims.

#47 · Legal

Pass when: Third-party logos and photography rights cleared for perpetual web use

Why: Stock licenses often cap impressions or prohibit logo compositing.

Verify: Asset registry links to license PDFs; Pexels/Unsplash brand guidelines respected; client logos under contract clause permitting case study usage.