ENGINEERING · CHECKLIST

API Design Checklist

Design consistent, evolvable APIs your team will thank you for.

NWARRAH

Systems, software & applied AI — engineered to last.

Use this checklist before shipping any public or internal API. It captures the decisions that are painful to reverse once clients depend on them.

Contract & Consistency

- [ ] Resource names are nouns, plural, and lowercase (e.g. /invoices).
- [ ] HTTP verbs match intent: GET (read), POST (create), PATCH (partial), PUT (replace), DELETE.
- [ ] Errors return a consistent shape: code, message, and details.
- [ ] Status codes are correct: 400 vs 401 vs 403 vs 404 vs 409 vs 422.
- [ ] Field naming convention is uniform (camelCase or snake_case — pick one).

Versioning & Evolution

- [ ] Versioning strategy chosen (URI /v1 or header) and documented.
- [ ] Additive changes only within a version; breaking changes bump the version.
- [ ] Deprecation policy and sunset headers defined.

Pagination, Filtering & Sorting

- [ ] List endpoints paginate by default (cursor preferred over offset).
- [ ] Filtering and sorting parameters are explicit and validated.
- [ ] Maximum page size enforced server-side.

Security

- [ ] Authentication method defined (OAuth2 / API key / JWT).
- [ ] Authorization checked per resource, not just per route.
- [ ] Rate limiting and quota headers returned.
- [ ] Input validated and sanitized on every endpoint.

Observability & Docs

- [ ] OpenAPI/Swagger spec generated and published.
- [ ] Every endpoint has example request and response.
- [ ] Structured logging with request IDs for tracing.
- [ ] Idempotency keys supported for unsafe retries.