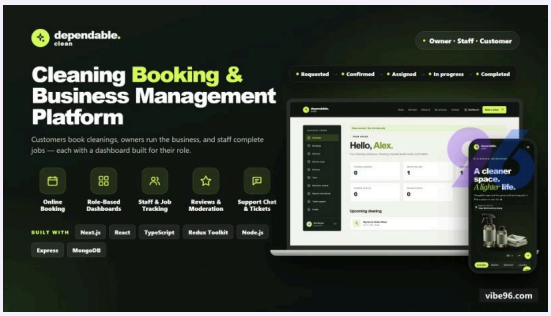
This report has been replaced by QR-26-00118 — a newer version of the product was reviewed.



VIBE96 QUALITY REPORT

Dependable-clean

Full-stack cleaning business platform with customer booking, staff dispatch and role-based dashboards

Product ID	**B0446-53515**
Builder	**Nishat Raihana Prantik**
Version reviewed	**1.3.0 · released 4 Nov 2026**
Stack	**Next.js 16.2 + React 19.3 (frontend), Express 5.1 (backend) · JavaScript (Node.js 20.13+) · MongoDB 6.20+**
Built with	**OpenAI Codex, Claude Code, GitHub Copilot**
Review period	**2 Nov 2026 – 4 Nov 2026**

74 / 100

Listed after a manual review

Pass mark 75 and no failing check.

Scores

Security	75
Code structure	62
Docs & completeness	73
Dependency health	72
Build & deploy	80

✓ **AI code audit**
6 checks · 2 Nov 2026

✓ **Installed & run**
4 Nov 2026

✓ **Demo vs delivered**
4 Nov 2026

✓ **Final sign-off**
4 Nov 2026

At a glance

- ✓ Installed and run from the delivered code — 8 of 8 checks answered yes.
- ✓ Live demo compared with the delivered code — 7 of 7 checks answered yes.
- ! 11 of 15 promised items delivered (setup guide, example config and the rest).
- ✓ Security scored 75/100 with no failing check.
- ! 6 open warnings — explained in part 1.

Check this report is genuine. Scan the code or open vibe96.com/report/QR-26-00096. The online copy always shows the latest status.

PART 1

AI code audit

The full source archive was read by our AI auditor against each check. It reads the code — it does not run it; running it is part 2.

CHECK	WHAT WE FOUND	SCORE	RESULT
Secrets & credentials	No real API keys, database URIs or signing secrets are committed. The .env.example uses placeholders and AUTH_SECRET falls back to a random value. However, demo account passwords are hardcoded in a project file and shown on the login page, so the demo admin (superAdmin) account could be a backdoor if demo mode stays enabled in production.	82	Warning
Dependency vulnerabilities	A single root package-lock.json exists (omitted from the digest, so contents are unverified) and the dependency set is mostly current. Caret ranges, an unmaintained upload middleware that is registered globally, and a few dependency-hygiene gaps keep this from a clean pass. No confirmed critical (RCE/auth bypass) advisory could be tied to the declared versions.	72	Warning
Authorisation & access control	Passwords use salted scrypt with timing-safe compare, and tokens are HMAC-signed with expiry. The visible routes use role guards (e.g. requireSuperAdmin on /addLocation), but index.js was truncated, so most mutating routes and id-based lookups could not be traced. Public demo credentials and a /demoLogin endpoint that can grant superAdmin are a production risk.	72	Warning
Database access rules	The visible backend uses the MongoDB driver with parsed ObjectIds and updates scoped by _id, email or setupHash, and no string-built queries appear. The digest truncates most of index.js and management.js, so the scoping of deletes and per-user queries could not be fully verified. The schema leaves out document validators, has no foreign keys or relational integrity, and some hot query fields are not indexed.	72	Warning
Code structure & duplication	The project is organised by workspace and has clear helper modules (auth, validation, permissions), but a project file concentrates routing, startup, persistence and business logic in one large file, and the frontend mirrors this with very large screen components. Configuration values such as the Dhaka timezone and demo credentials are hard-coded in several places, and the demo accounts are duplicated between backend and frontend.	62	Warning
Build reproducibility	The npm workspace, root lockfile, engines field and scripts are coherent, and a clean machine should be able to install, build and test. HowToSetup.md was not in the digest, so its prerequisites and step order could not be verified. A stale README reference, a build script that does not type-check the backend, and an unpinned Next.js version are small gaps.	80	Warning

Open warnings

Problems that did not stop the listing. They stay on the product page until a later version fixes them.

Warning 1 **No real credentials found; demo passwords are hardcoded and published in source and UI**

No real API keys, database URIs or signing secrets are committed. The .env.example uses placeholders and AUTH_SECRET falls back to a random value. However, demo account passwords are hardcoded in a project file and shown on the login page, so the demo admin (superAdmin) account could be a backdoor if demo mode stays enabled in production.

Warning 2 **Backend index.js is a god file mixing routes, auth, DB and business rules; several files are oversized**

The project is organised by workspace and has clear helper modules (auth, validation, permissions), but a project file concentrates routing, startup, persistence and business logic in one large file, and the frontend mirrors this with very large screen components. Configuration values such as the Dhaka timezone and demo credentials are hard-coded in several places, and the demo accounts are duplicated between backend and frontend.

Warning 3 **Workspace builds look sound; setup doc unverified and a few stale references and gaps**

The npm workspace, root lockfile, engines field and scripts are coherent, and a clean machine should be able to install, build and test. HowToSetup.md was not in the digest, so its prerequisites and step order could not be verified. A stale README reference, a build script that does not type-check the backend, and an unpinned Next.js version are small gaps.

Warning 4 **Passwords hashed and guards present on visible routes, but most of the API is unverifiable and demo logins are risky**

Passwords use salted scrypt with timing-safe compare, and tokens are HMAC-signed with expiry. The visible routes use role guards (e.g. requireSuperAdmin on /addLocation), but index.js was truncated, so most mutating routes and id-based lookups could not be traced. Public demo credentials and a /demoLogin endpoint that can grant superAdmin are a production risk.

Warning 5 **Lockfile present, but caret ranges and unmaintained express-fileupload need attention; no known critical CVE verifiable**

A single root package-lock.json exists (omitted from the digest, so contents are unverified) and the dependency set is mostly current. Caret ranges, an unmaintained upload middleware that is registered globally, and a few dependency-hygiene gaps keep this from a clean pass. No confirmed critical (RCE/auth bypass) advisory could be tied to the declared versions.

Warning 6 **No injection seen in visible code, but much of the backend was truncated and several schema gaps remain**

The visible backend uses the MongoDB driver with parsed ObjectIds and updates scoped by _id, email or setupHash, and no string-built queries appear. The digest truncates most of index.js and management.js, so the scoping of deletes and per-user queries could not be fully verified. The schema leaves out document validators, has no foreign keys or relational integrity, and some hot query fields are not indexed.

Requirement list

What the builder agreed to deliver before uploading — 11 of 15 met.

✓	Complete source for every component	Met
✓	No real credentials in the archive	Met
!	Builds from a clean machine	Partial
✓	Database script or migrations	Met
!	Authentication and roles on every mutating endpoint	Partial
!	Pinned dependencies without critical CVEs (nice)	Partial
✓	Documentation set (nice)	Met
!	Working live demo	Partial
✓	README.md	Met
✓	HowToSetup.md	Met
✓	CLAUDE.md (or AGENTS.md) (nice)	Met
✓	CHANGELOG.md (nice)	Met
✓	.env.example	Met
✓	a project file	Met
✓	a project file (nice)	Met

PART 2

Human review

Reviewers from the Vibe96 team in Dubai worked through each question below; a final reviewer signed it off.

Stage 1 — Installed and run from the delivered code

Completed 4 Nov 2026

A reviewer installed the product on a clean machine, following only the guide that ships with it.

QUESTION	ANSWER	REVIEWER'S NOTE
Packages restored without errors	Yes	
Solution builds clean	Yes	
Database created from the shipped script or migrations	Yes	
First sign-in works with the documented steps	Yes	
Setup guide is accurate and complete	Yes	
Every module in the feature list opens and works	Yes	
No real secrets in the archive	Yes	
Branding and company details can be changed without code	Yes	

Stage 2 — Live demo compared with the delivered code

Completed 4 Nov 2026

A second reviewer checked that what the listing and demo show is what the buyer receives.

QUESTION	ANSWER	REVIEWER'S NOTE
Demo URL is reachable	Yes	
Demo credentials work	Yes	
Demo runs the same version as the archive	Yes	
All five differentiators are visible in the demo	Yes	
Screenshots match the demo	Yes	
Nothing in the demo is missing from the code	Yes	
Datasheet claims are accurate	Yes	

Changes asked for during review

None — approved on the first round.

Sign-off: approved for sale on 4 Nov 2026 with 6 warnings shown publicly.

What this report covers — and what it doesn't

- **It covers** version 1.3.0 exactly as the buyer downloads it: the source archive, the setup guide and the live demo on the dates above.

- **It is not** a penetration test, a performance or load test, or a legal review of third-party package licences.
- **Scores are a point in time.** Libraries age; a later version is audited again and gets its own report.
- **Your setup matters.** Hosting, configuration and changes made after purchase are outside this review.
- **How the score is made:** each AI check is scored 0–100 and weighted (security counts most). A listing needs 75 or more, no failing check, and the human review passed.
- **Always try the live demo** before buying, and ask the builder questions from the product page.

Report history

REPORT	VERSION	DATE	SCORE	STATUS
QR-26-00118	1.8.2	11 Nov 2026	**86**	Current
QR-26-00096	1.3.0	4 Nov 2026	**74**	Replaced
QR-26-00077	1.0.0	28 Oct 2026	**0**	Replaced