Halal Certification Website Requirements (v2)

1 Overview & Objective

Create a **Progressive Web App (PWA)** that enables shop owners to apply for halal certification, inspectors to review and approve applications, and the public to verify certification status. The site must operate seamlessly on desktop, iOS, and Android—installable, offline-capable, and push-notification ready.

---

2 Functional Requirements

2.1 User Roles & Permissions

Role	Authentication	Key Privileges
Visitor	none	Scan QR / search stores, view certification, submit feedback (pending moderation)
Applicant (Shop Owner)	none	Submit application form, receive email updates, download/print QR code
Inspector	login required	Access inspector dashboard, view/approve/reject applications, schedule site visits, upload inspection notes
Admin	login required	All inspector rights + manage users, moderate feedback, revoke/renew certificates, view analytics

2.2 Core User Stories

1. **Application submission** – As a shop owner, I fill out a form without logging in and receive email confirmation.
2. **Inspection & review** – As an inspector, I log in, review applications, visit the store, and record findings.
3. **QR issuance** – If approved, the system emails a QR code (Model 2, Version 4, alphanumeric) to the owner.
4. **Public verification** – As a visitor, I scan the storefront QR (or search by name/address) to see live status.
5. **Feedback & complaints** – As a visitor, I leave a review or complaint; it is private until an admin approves it.

2.3 Pages / Components

- **Home** – Mission, CTA to verify certification, search bar.
- **About Us** – Background, key personnel, FAQs.
- **Contact Us** – Web form, map, support email, phone.
- **Terms & Privacy** – User agreement, privacy policy, data‑retention summary.
- **Application Form** – Multi‑step, email confirmation, file uploads (e.g., business license).
- **Inspector Dashboard** – Application queue, status filters, audit log, decision actions.
- **Store Certificate Page** – Public view with store details, certification status, expiry date, last inspection.
- **Feedback Hub** – List + moderation queue, category filters, admin approval toggle.

---

3 Non‑Functional Requirements

Aspect	Requirement
PWA	Must score ≥ 90 on Lighthouse PWA audits; responsive ≤ 2 s FCP on 3 G.
Security	HTTPS everywhere, OAuth2/JWT for logins, rate‑limit QR scans (≤ 60/min/IP), reCAPTCHA on public forms.
Performance	Search latency ≤ 300 ms for 10 k stores; use indexed full‑text search.
Accessibility	WCAG 2.2 AA compliance; RTL layout ready (Arabic).
Internationalisation	English (default) + Arabic; JSON i18n files.
Scalability	Architecture must support 100 k certificates, 1 M monthly QR scans; horizontal DB read replicas.
Audit Logging	Immutable logs for application status changes, inspector actions, feedback moderation.
Privacy	Comply with Australian Privacy Principles & GDPR: data stored in AU‑based region, 5‑year retention cap, deletion on request.

---

4 Data & Integration Specs

Entity	Key Fields
Store	id, name, address, geo‑coords, contact, ownerEmail
Certificate	id, storeId, status {pending, approved, revoked}, issuedDate, expiryDate, inspectorId

Inspection	id, certificateId, notes, visitDate, decision
Feedback	id, storeId, authorEmail (optional), content, type {review, complaint}, status {pending, approved, rejected}, createdAt

- **Email** – Use transactional service (e.g., AWS SES) with DKIM/SPF; templates: application-received, update, approved+QR, rejected, renewal-reminder.
- **QR Payload** – `https://example.com/cert/<certificateId>`; shortlinks via branded domain.
- **Moderation Workflow** – Feedback status defaults to *pending* → *approved* or *rejected* by Admin; auto-notify submitter on decision (if email provided).
- **Re‑certification** – Certificates expire after 12 months; system emails owner 30/7 days before.
- **Analytics/KPIs** – Track: avg time to approve, unique QR scans, complaints resolved, Lighthouse scores.

---

5 Acceptance Criteria

1. **PWA installable** on Chrome, Safari, Firefox mobile with offline fallback page.
2. **Application form** submits successfully on desktop & mobile; applicant receives confirmation email within 1 min.
3. **Inspector decision** updates certificate status; audit log records userId, timestamp, IP.
4. **QR scan** from a low‑end Android loads certificate page < 2 s on 3 G.
5. **Feedback** cannot appear publicly without admin approval.
6. **Accessibility** verified via automated aXe tests, manual keyboard nav review.

---

6 Implementation Roadmap (high‑level)

Phase	Scope
MVP	Application flow, inspector dashboard, QR generation, basic PWA shell.
Phase 2	Search enhancements, feedback moderation UI, bilingual UI.
Phase 3	Analytics dashboard, notification center, locator map, push notifications.

---

7 Open Questions

1. Certification fee processing required (online payments)?
2. Inspector identity verification (2FA)?
3. Do we need public API access for third-party apps?

Email integration via Amazon SES or Mailgun