Icebreaker Alert

A trusted alert and coordination network for nonprofits operating in civil emergencies — secure, browser-based, and independent of corporate app stores.

About Icebreaker Alert

Icebreaker Alert is a browser-based alert and coordination system built for **civil emergencies** — times when Wi-Fi and hotspots still work, but **trust and access have broken down.**

It's designed for **nonprofits, mutual-aid groups, and civic organizations** that need to distribute verified alerts during protests, curfews, or information blackouts — when mainstream platforms throttle, censor, or de-prioritize communication.

There's no app to install, no app store to rely on, and no personal data collected. Icebreaker runs entirely in **Google Chrome**, using built-in GPS and nearby Wi-Fi signals to pinpoint location accurately while preserving anonymity.

Because it's **open source** and **platform-independent**, it stays functional even when corporate or government systems restrict access.

Goal: provide civil-society groups with a secure, controllable way to broadcast verified alerts in real time over ordinary Wi-Fi networks.

Why It Exists

Open community alert platforms collapse under disinformation and spam during unrest. Social media adds algorithmic throttling, surveillance risk, and noise.

Icebreaker Alert creates a **closed, verified network** where only approved participants can issue messages — bridging the gap between public social platforms and private coordination tools. It's designed for environments where **connectivity exists but institutional trust does not.**

Key Benefits for Nonprofits

- **Browser-based (Chrome only)** — no app installation required.
- **Verified alerts only** — prevents spoofing and false data.
- **Wi-Fi/hotspot ready** — works on existing local networks.
- **Accurate location** — uses GPS + Wi-Fi data.
- **Independent** — not tied to Apple, Google Play, or mobile carriers.
- **Low-cost, self-hosted, and scalable** — ideal for NGOs and civic groups.

How It Works

1. Volunteer Alerters (Physical Beacons)

Authorized volunteers receive a **QR code card** with a unique, secure URL and a **Yubikey (NFC key)** to trigger verified alerts directly through Chrome.

- Nonprofits can issue or revoke volunteers instantly.
- Redirects can be updated remotely if servers move.
- No personal data — only anonymous hashed IDs.
- **Admin messaging**: When creating alerts, authorized users can include:
  - **S.A.L.U.T.E. Protocol Reporting** — Structured incident details (Size, Activity, Location, Unit, Time, Equipment) via a dedicated modal.
  - **Custom messages** — Situation-specific instructions (e.g., "Avoid Main Street, use side streets").
  - **Info URLs** — Links to detailed coordination pages (e.g., `https://www.alertpage.com`).
  - **Auto-fill** — Time and location are automatically populated based on the user's context.
  - Severity levels removed per user feedback — focus on binary alert/no-alert model

2. Scout Devices

Low-cost **ESP32 "Scout" devices** receive and verify alerts with built-in alarm capabilities.

- **Portable design**: Includes lanyard for wearing or hanging in strategic locations
- **Wi-Fi connectivity**: Operates over Wi-Fi networks, including phone hotspots for mobile deployment
- **No cellular dependency**: Works entirely over Wi-Fi, ideal for areas with limited cellular coverage
- **Wi-Fi fingerprint positioning**: Uses BSSID scanning (no GPS required) to achieve 20–50 m location accuracy
- **2-mile alert radius**: Devices are notified when within 2 miles of an active alert
- **Rich alert data**: Receives distance to nearest alert (rounded to 0.5-mile increments for privacy), custom messages, and action URLs
- **Built-in alarm**: Audio alerts notify nearby individuals when emergencies are detected
- **Flexible deployment**: Ideal for job sites, offices, observation points, safehouses, or carried by field volunteers
- Target cost: **under $15** per unit in production

Polling Architecture & Timing:

- Scout devices do not receive or transmit real-time data
- Each unit wakes from low-power mode every 15 minutes to check a nonprofit-controlled endpoint for any active alerts
- This design prevents continuous communication and limits alert freshness
- The developer does not control or host any alert servers
- Timing behavior is fixed in firmware and chosen for battery preservation and to ensure the system cannot function as a real-time tracker
- Scouts cannot originate alerts; they only poll for status

3. Alert Response System

When devices check for alerts via the `/status` endpoint or browser interface:

- **2-mile notification radius**: Alerts trigger for devices within 2 miles of the alert origin point
- **Distance awareness**: Devices and users learn how far they are from the nearest alert (rounded to 0.5-mile increments for privacy)

- **Custom messaging**: Admins provide situation-specific instructions or safety information visible to all nearby devices
- **Action URLs**: Alerts include links to coordination resources (e.g., `https://www.alertpage.com` for future local network access)
- **Location awareness**: Status endpoint returns the device's reverse-geocoded address (via MapTiler) so Scouts can display "Your Estimated Location"
- **Privacy-preserving**: Device locations are calculated but not stored or logged — only distance to nearest alert is provided
- **Modern UI**: Clean Tailwind CSS interface with **full bilingual support (English/Spanish)**.
    - Dynamic language switching without page reloads.
    - Deep linking support (e.g., `?lang=es`).
    - Integrated "Reporting Guide" available in both languages.
- **Browser interface**: Users see custom messages, info URLs, distance, and expiration times in a professional, accessible design
- **ESP32 Scouts** (when implemented): Display location awareness, simplified alerts with audio/visual indicators

4. Integration with Existing Hotlines

Nonprofits with **established crisis hotlines** can integrate verified reports directly into Icebreaker's alert database.

- API endpoints accept authenticated submissions from trusted hotline systems
- Operators can forward geolocated tips or verified field reports in real time
- Minimal customization needed — hotline data feeds map to Icebreaker's alert schema
- Preserves existing workflows while extending reach to browser and Scout device networks
- Ideal for organizations with 24/7 call centers or text-based tip lines *(Custom integration support available — contact us for nonprofit partnership details.)*

5. Future: Digital Beacons (Social Media Integration)

Vetted **social media accounts** — for example, verified field reporters or partner organizations on **Bluesky, Mastodon, or X** — can act as *digital beacons*.

- Their posts containing GPS coordinates could be ingested automatically.
- Each account must be pre-approved and cryptographically verified to prevent spoofing.
- This enables a **hybrid trust model**: human-verified sources plus automated signal ingestion. *(Feature in active research and planned for future releases.)*

6. Future: Local Network Coordination (icebreaker.local)

When multiple ESP32 Scouts are connected to the same Wi-Fi network (including phone hotspots), planned features include:

- **Smart discovery page**: Visit `http://icebreaker.local` to see a list of all Scout devices on the network
    - If only one Scout detected, auto-forward to its configuration page
    - If multiple Scouts present, show device list with IDs and signal strength

- **Per-device configuration**: Each Scout accessible via unique hostname (e.g., `icebreaker-scout-abc123.local`)
- **Detailed alert viewing**: Access admin-provided status updates, custom messages, and situation-specific instructions
- **mDNS service discovery**: Scouts advertise `_icebreaker._tcp.local` for automatic network discovery *(Requires ESP32 firmware implementation — planned for future release)*

Technical Stack

- **Backend**: Rust (Actix-web)
  - **Templating**: Tera (Jinja2-like)
  - **Persistence**: Simple JSON file storage (no database required)
  - **Geolocation**: Google Geolocation API (WiFi) + MapTiler (Reverse Geocoding)
  - **Offline Logic**: `tzf-rs` for local timezone resolution
- **Frontend**: Vanilla JavaScript + Tailwind CSS
  - **I18n**: Client-side translation object with URL parameter state
  - **Styling**: Utility-first CSS via Tailwind CLI
- **Deployment**: Docker containerized (Alpine Linux base)

Security and Privacy

- No personally identifiable information (PII) collected or stored.
- ESP32 Scouts use private keys for message authentication.
- Volunteers represented only by hash IDs.
- Nonprofits can maintain **air-gapped volunteer lists.**
- Search engines blocked via robots.txt and noindex meta tags.
- Digital beacon ingestion from verified social media accounts (users need to be vetted and their PII could be exposed)
- User-configurable endpoints for ESP32 Scouts
- Admin dashboard for QR and volunteer management
- Signed payload verification
- Continued anti-censorship and privacy hardening

License