TruthFirst Media - Cybersecurity Spec

1. Wallet & Token Handling

- Use Solana Wallet Adapter for secure wallet connections.

- Validate wallet connections using signed messages.

- Apply token balance checks for gating reports, merch, and voting.

- Use snapshot logic for anti-Sybil voting verification.

2. Content Submission Security

- Enforce file type/size restrictions (PDF, JPG, PNG only).

- Scan uploaded files using Cloudinary or VirusTotal APIs.

- Sanitize all file names to prevent injection attacks.

3. Authentication & Rate Limiting

- Apply CAPTCHA on all public forms.

- Limit form submissions per wallet/IP using Firebase or Cloudflare.

- Throttle uploads and voting endpoints.

4. Smart Contract Security

- Contract audits via CertiK or Code4rena.

- Renounce ownership post-deployment (optional).

- Control max tx %, cooldowns, and whitelist phases early.

5. Frontend/API Security

- Escape all user-generated content on render.

- Force HTTPS, secure cookies, and scoped CORS headers.

- Protect admin routes and panel logic.

6. Monitoring & Incident Response

- Integrate Sentry for frontend monitoring.

- Track wallet behavior using Helius/SolanaFM.

- Enable DAO emergency flag votes (freeze subsystems if compromised).