TruthFirst Media - Secure Report File Management

Purpose

Outline security measures for managing both user-submitted tips and distributed premium reports, ensuring encrypted, verifiable access and long-term integrity.

Tools & Platforms

- IPFS: Decentralized, tamper-proof hosting for purchased reports.
- Cloudinary: Tip file uploads with moderation and auto-expiry.
- Firebase/Supabase: Store metadata, access tracking, and secure links.
- Privy or Lit Protocol: Token-gated, wallet-decrypted access to PDFs.
- VirusTotal or Cloudflare: Scanning tool for malicious upload detection.

Workflow: Tip Submissions

- 1. File uploaded via secure form (Cloudinary or Firebase).
- 2. Virus/malware scan triggered.
- 3. Metadata stored with optional pseudonymous wallet.
- 4. Staff receives secure alert.

Workflow: Report Unlock

- 1. Report hosted on IPFS or secure CDN.
- 2. User connects wallet.
- 3. System verifies $ANTY holdings via SPL check.
- 4. Unlock access delivered via signed link or gated viewer.
- 5. Optional watermarking with wallet ID.

Best Practices

- Allow only PDF uploads for tips or final reports.
- Auto-expire unused file URLs after 2472 hours.
- Use rate limits on uploads and report downloads.
- Add watermarking for internal team handling sensitive leaks.
- Route all actions through audit-logged backend endpoint.