**ELECTA - Final API Security & Rate-Limiting Policy (v1.2)**

**Date:** July 25, 2025

**Status:** Finalized & Approved for MVP Development

**Objective**

To define the finalized, actionable rules that enforce the Robust Security, Disinformation & Abuse Mitigation, and Data Ethics principles for the MVP launch. This document serves as the primary security reference for development and operations.

**1. Authentication & Registration Endpoints**

* **Endpoints:**
  + POST /api/v1/auth/register/request-otp
  + POST /api/v1/auth/register/verify-otp
  + POST /api/v1/auth/login
* **Final Policies:**
  1. **OTP Rate Limit (Frequency):** Enforce a limit of **1 request per 60 seconds** per unique mobile number or IP address.
  2. **OTP Rate Limit (Daily Cap):** Enforce a hard limit of **5 OTP requests per day**. This is a collective cap triggered if *either* the mobile number or the IP address hits the threshold.
  3. **Brute-Force Protection (Progressive Lockout):** After **5 consecutive failed login or OTP verification attempts**, the corresponding account or IP address will be locked for **15 minutes**. A second lockout within 24 hours will trigger a longer lockout of **1 hour**.
  4. **IP Reputation Filtering:** A Web Application Firewall (WAF) will be used to block requests originating from known malicious IPs or anonymous proxies.
  5. **Audit Logging:** All failed authentication attempts will be logged to the AuditLogs table for security monitoring.

**2. NID Verification Endpoints**

* **Endpoints:**
  + POST /api/v1/user/verification/nid-submit
  + GET /api/v1/user/verification/status
* **Final Policies:**
  1. **Authorization:** The nid-submit endpoint is restricted to users with Mobile-Verified status (Level 1) or higher.
  2. **Submission Rate Limit:** Limit users to **2 submission attempts per 24-hour period**.
  3. **Payload & File Type Validation:** The API Gateway will enforce a **5MB file size limit** and a strict MIME type whitelist, accepting only image/jpeg and image/png.
  4. **CAPTCHA Integration:** After the first failed submission attempt within a 24-hour period, any subsequent attempt from that user must be protected by a CAPTCHA.
  5. **Status Check Rate Limit:** To prevent polling abuse, the GET /user/verification/status endpoint will be rate-limited to **10 requests per hour** per user.

**3. Public Q&A Interaction Endpoints**

* **Endpoints:**
  + POST /api/v1/questions
  + POST /api/v1/questions/{id}/upvote
* **Final Policies:**
  1. **Authorization:** POST /questions is restricted to NID-Verified users (Level 2). POST /.../upvote is restricted to Mobile-Verified users (Level 1) or higher.
  2. **Question Rate Limit:** Limit submissions to **1 per NID-verified user, per candidate, per 24 hours**.
  3. **Upvote Rate Limit:** Limit upvote actions to **10 per user per minute**.
  4. **Input Validation:** The API will strictly enforce Content-Type: application/json headers and the 500-character limit on question submissions.
  5. **Offender Logging:** Users who repeatedly trigger rate limits will be flagged for administrative review.

**4. Admin Panel Endpoints**

* **Endpoints:**
  + All endpoints under /api/v1/admin/...
* **Final Policies:**
  1. **IP Whitelisting:** Access to all Admin Panel endpoints will be restricted by an IP address whitelist. Only IP addresses belonging to the secure office network or approved VPNs will be allowed to connect.
  2. **General Rate Limit:** To prevent abuse from a compromised admin account, a general rate limit of **60 requests per minute** will be applied to all authenticated admin users.

**5. Platform-Wide Security & Hardening Policies**

1. **API Versioning:** All API endpoints are versioned from launch (/api/v1/...) to ensure non-disruptive updates.
2. **CORS Policy:** A strict Cross-Origin Resource Sharing (CORS) policy will be enforced to only allow requests from our approved web domains.
3. **CSRF Protection:** All state-changing requests originating from web clients will be protected by an anti-CSRF token mechanism.
4. **JWT Token Expiry:** User session JWTs will have a validity of **1 hour**, with a secure refresh token mechanism.
5. **HTTPS Enforcement (HSTS):** The platform will use HSTS (HTTP Strict Transport Security) headers to enforce secure connections.
6. **Input Sanitization:** All user-submitted text fields will be sanitized on the backend to strip potential HTML or script payloads (XSS mitigation).
7. **Idempotency Keys:** All critical POST requests (e.g., /nid-submit, /questions) will support an Idempotency-Key header to prevent accidental double submissions caused by unstable mobile networks.

**6. Phase 2 Security Considerations**

This section serves as a placeholder for future security enhancements.

* **Public Challenge System:** Will require its own set of rate limits and authorization rules for Level 3 "Trusted Contributors".
* **AI-Driven Anomaly Detection:** Implement machine learning models to detect unusual patterns in user behavior beyond simple rate limits.
* **Mobile App Attestation:** Integrate Google Play Integrity or similar services to ensure API requests originate from the legitimate, untampered mobile application.