**ELECTA - Operational Runbook (v1.1)**

**Document Version:** 1.1 **Date:** July 29, 2025 **Status:** Approved

**1.0 Introduction**

This document provides a set of Standard Operating Procedures (SOPs) for the ELECTA operations and technical teams. Its purpose is to ensure a swift, consistent, and effective response to common operational incidents, security events, and service outages. This is a living document and will be updated as the platform evolves.

**2.0 Alerting Channels & Triage**

* **Primary Alerting Channel:** All automated alerts from the monitoring systems (e.g., Grafana, Prometheus Alertmanager, Sentry) will be routed to a dedicated #electa-alerts Slack channel and sent via email to a designated operations distribution list.
* **First Responders:**
  + **Operational Alerts** (e.g., high verification queue, moderation spikes): The on-duty Super Admin or a designated team lead is the first responder.
  + **Technical Alerts** (e.g., API downtime, high error rates): The on-call Backend Developer is the first responder.

**3.0 Incident Response Procedures**

**3.1 Incident: NID Verification Queue Exceeds Red SLA (>500 Pending)**

* **Detection:** The monitoring system (SEC-1) triggers an automated alert when the number of citizen profiles in PENDING\_NID status exceeds 500.
* **Triage (First Responder: Super Admin):**
  + Acknowledge the alert in the #electa-alerts channel.
  + Access the Admin Panel to verify the current queue size and the rate of new submissions.
  + Assess the number of currently active Verification Officers.
* **Response Protocol:**
  + **Activate Backup Staffing:** The Super Admin will immediately initiate the "Peak Scaling" plan by contacting the pre-vetted pool of temporary staff to log in.
  + **Communicate Internally:** Announce in the main team channel that the platform is in a "high-load" state for NID verifications.
  + **Monitor Queue Health:** Continuously monitor the queue size and processing rate until the count returns to the "Yellow" SLA tier (< 500).

**3.2 Incident: External SMS Gateway (OTP) Service Failure**

* **Detection:** Monitoring system detects a spike in 5xx errors or timeouts from the /api/v1/auth/request-otp endpoint.
* **Triage (First Responder: On-call Developer):**
  + Acknowledge the alert.
  + Immediately check the official status page of our external SMS provider (e.g., Twilio, SendGrid).
* **Response Protocol:**
  + **If Provider Confirms Outage:**
    - Post a pre-written "System Status" banner on the app's login and registration screens.
    - Continuously monitor the provider's status page for updates.
    - Once the provider resolves the issue, run a test to confirm OTPs are being delivered, and then remove the status banner.
  + **If Provider Shows No Outage:**
    - Escalate to a senior backend developer.
    - Inspect application logs (LOG-1) and cloud provider network configurations for internal issues.

**3.3 Incident: Unplanned Downtime of a Core Service (API, Database)**

* **Detection:** External uptime monitor (e.g., Pingdom) and internal system alerts detect that the API Gateway is unresponsive or returning a high rate of 5xx errors.
* **Triage (First Responder: On-call Developer):**
  + Acknowledge the page/alert immediately.
  + Attempt to access the API health check endpoint.
* **Response Protocol:**
  + **Diagnose:** Access the cloud provider console (AWS/GCP) and the centralized logging system to identify the root cause.
  + **Communicate:** Post a "System Status" banner.
  + **Resolve:** If it's a crashed container, restart the service. If it's related to a recent deployment, initiate a rollback to the last known stable version.
  + **Verify:** Once the service is restored, perform a sanity check to ensure core functionality is working.
  + **Remove Banner:** Deactivate the public status message.

**3.4 Incident: Coordinated Spam/Abuse Attack Detected**

* **Detection:** Monitoring system alerts on an unusually high rate of triggered API rate limits, or a sudden spike in spammy Questions from new, similar accounts.
* **Triage (First Responder: Super Admin / Moderator):**
  + Acknowledge the alert.
  + Review monitoring dashboards to identify the attack pattern.
* **Response Protocol:**
  + **Block Malicious Actors:** Use the Web Application Firewall (WAF) to block the offending IP ranges.
  + **Increase Aggressiveness:** Temporarily lower the rate limits on the targeted endpoints.
  + **Clean Up:** Use the Admin Panel to bulk-suspend the identified spam accounts and hide/delete the spam content.

**3.5 Incident: Disputed Charter Compliance Assessment (New)**

* **Detection:** A formal complaint is received from a political party via an official contact channel, or a concern is raised internally by the Advisory Board.
* **Triage (First Responder: Super Admin):**
  + Acknowledge receipt of the dispute to the complainant within 12 hours.
  + Verify the complainant's identity and standing.
  + Access the Admin Panel, locate the specific PartyComplianceRecord, and review the linked evidence and the Data Editor's assessment notes.
* **Response Protocol:**
  + **Isolate Record:** Immediately update the compliance\_status of the record in question to UNDER\_REVIEW. This status and a note indicating the dispute will be visible on the public-facing site.
  + **Compile Case File:** Gather all relevant information: the original assessment, the evidence used, the editor's notes, the new complaint, and any counter-evidence provided.
  + **Escalate:** Escalate the complete case file to the **Community Advisory Board** for a formal, independent review.
  + **Implement Ruling:** Upon receiving the board's final decision, the Super Admin will update the PartyComplianceRecord with the new status and add the board's official reasoning to the public\_notes field for full transparency.
  + **Communicate Resolution:** Formally communicate the final decision and the public-facing changes to the original complainant.

**4.0 Escalation Paths**

| Incident Type | Level 1 (First Responder) | Level 2 (Escalation) | Level 3 (Final Authority) |
| --- | --- | --- | --- |
| High Verification Queue | Super Admin | Head of Operations | Project Lead |
| Service Outage | On-call Developer | Lead Developer | Head of Engineering |
| Security Attack | Super Admin | Lead Developer | Head of Engineering / Project Lead |
| **Disputed Compliance Assessment (New)** | **Super Admin** | **Community Advisory Board** | **Community Advisory Board** |

Export to Sheets

**5.0 Post-Mortem Process**

For any incident classified as "Red" (e.g., service downtime > 5 minutes, NID queue breach > 2 hours), a formal, blameless post-mortem will be conducted within 48 hours. The goal is to identify the root cause of the incident and create actionable tickets to improve system resilience and prevent recurrence.