SHARED ALERT PROTOCOL FOR DIGITAL RIGHTS INCIDENTS

Uganda General Elections 2026

Adopted by: Unwanted Witness (UW) and Women of Uganda Network (WOUGNET).
Convened by: Unwanted Witness
Date of Adoption: 23rd December, 2025
Status: Operational Protocol

1. PURPOSE AND OBJECTIVES

This Shared Alert Protocol establishes a coordinated, timely, and rights-based mechanism for detecting, verifying, communicating, and responding to digital rights incidents, particularly internet shutdowns and network disruptions, before, during, and after Uganda's 2026 General Elections.

The Protocol aims to:

- Enable early detection of digital disruptions.
- Ensure accurate and verified information sharing.
- Coordinate rapid, proportionate, and safe responses.
- Minimise harm to freedom of expression, access to information, and electoral integrity.
- Strengthen accountability and evidence generation.

2. SCOPE OF THE PROTOCOL

This Protocol applies to digital rights incidents, including but not limited to:

- Full or partial internet shutdowns.
- Bandwidth throttling.
- Platform-specific blocking (social media, messaging apps).
- SMS, voice, or data disruptions.
- DNS blocking or IP filtering.
- Election-related online content restrictions.

Temporal Scope:

- Pre-election period (campaigns).
- Election days.
- Post-election period (results and aftermath).

3. GUIDING PRINCIPLES

All actions under this Protocol shall be guided by:

- Respect for constitutional and international human rights standards.
- Accuracy and verification before public escalation.
- Do-no-harm and safety-first approaches.
- Transparency and accountability.
- Collaboration and non-duplication among partners.

4. ROLES AND RESPONSIBILITIES

4.1 Protocol Secretariat

Unwanted Witness shall serve as the Protocol Secretariat and is responsible for:

- Coordinating alerts and responses
- Maintaining secure communication channels
- Validating information and escalation decisions
- Documenting incidents for advocacy, litigation, and reporting

4.2 Participating Actors

Unwanted Witness (UW) and Women of Uganda Network (WOUGNET).

5. DETECTION AND VERIFICATION FRAMEWORK

5.1 Detection Sources

Incidents may be detected through:

- NetBlocks, OONI, BGP monitoring tools.
- ISP dashboards (where accessible).

- Crowdsourced user reports.
- Media and journalist observations.
- On-the-ground CSO monitoring

5.2 Verification Standards

An incident shall be considered **Verified** when:

- Confirmed by at least two independent sources; or
- Supported by one trusted technical measurement tool plus corroborating user or media reports.

Unverified incidents remain **Preliminary Alerts** until confirmation.

6. ALERT LEVELS AND TRIGGERS

Alert Level	Trigger	Description
Level 1: Watch	Early warning signals	Policy statements, minor anomalies
Level 2: Alert	Partial disruptions	Throttling, localised outages
Level 3: Critical	Severe disruptions	Nationwide shutdowns, platform blocking

7. INFORMATION FLOW AND ESCALATION LADDER

1. **Detection –** Incident identified by partner or UW monitoring
2. **Verification –** Cross-checking by UW and WOUGNET ICT & Programs teams
3. **Internal Alert –** Secure notification to Coordination Group
4. **Decision Point –** Determine escalation level
5. **External Response –** Legal, media, advocacy, or international escalation

Maximum verification time during high-risk periods: 30–60 minutes

8. RESPONSE PATHWAYS

8.1 Legal Response

- Demand letters to authorities.

- Court filings or injunctions.
- Engagement with regulators.

8.2 Media & Public Communication

- Pre-approved holding statements.
- Press briefings coordinated through UW.
- Responsible messaging to avoid panic or misinformation.

8.3 International Advocacy

- Alerts to regional and global partners.
- Diplomatic and multilateral engagement.
- Documentation for international mechanisms.

8.4 Telecom Engagement

- Direct engagement with service providers.
- Clarification of legal basis and scope.

9. PROTECTION AND SAFETY MEASURES

- Secure communication channels (Signal, encrypted email).
- Anonymisation of sensitive sources.
- Digital security guidance for journalists and activists.
- Risk assessment before naming individuals or locations.

10. DOCUMENTATION AND EVIDENCE MANAGEMENT

All incidents shall be documented using:

- UW Government & Regulatory Monitoring Tracker.
- UW Technical Disruption Tracker.

Evidence may include:

- Screenshots, logs, charts.
- Audio/video recordings.

- User testimonies.

11. COORDINATION MECHANISMS

- Digital Rights Coordination Group (Unwanted Witness (UW) and Women of Uganda Network (WOUGNET)).
- Secure real-time communication channel.
- Weekly coordination calls during high-risk periods.
- Emergency meetings during Level 3 alerts.

12. REVIEW, ADAPTATION, AND ACCOUNTABILITY

- Protocol effectiveness reviewed post-election.
- Lessons integrated into UW's Post-Election Internet Shutdown Impact Report.
- Recommendations used for policy and legal reform advocacy.

13. ADOPTION AND COMMITMENT

This Shared Alert Protocol is adopted on a voluntary basis by ***Unwanted Witness (UW) and Women of Uganda Network (WOUGNET)***, affirming their commitment to coordinated, responsible, and rights-based action to protect digital freedoms during Uganda's 2026 General Elections.

Signed / Endorsed by:



Unwanted Witness



Women of Uganda Network