KEEL — Keep Evil Enterprises Leveled

Document status: Approved

System name: KEEL — Keep Evil Enterprises LEVELED
System type: Prevention, detection, disruption-support, and coordination system for sexual exploitation enterprises
Owner: NATIONAL FEDERATION OF MENDOCINO
Version: 1.0 Draft

Procedure: The Sexual Exploitation Enterprise Prevention Act
Classification: Internal — Sensitive

> **Notice:** This document is a system charter, not legal advice. KEEL does not create law-enforcement authority, does not authorize vigilante action, and must operate only under applicable law, partner agreements, and approved policy. THIS PROVISION IS FOR THE Sexual Exploitation Enterprise ACT

---

1. Purpose

KEEL is a prevention and disruption-support system designed to help authorized organizations **detect, validate, disrupt, deter, and prevent sexual exploitation enterprises** as defined in the supplied legal definition.

KEEL's purpose is to:

1. Receive and triage reports and referrals involving suspected sexual exploitation enterprises.
2. Classify suspected activity against the legal elements of a "sexual exploitation enterprise."

3. Identify patterns, entities, relationships, and commerce nexuses requiring human review.
4. Route validated matters to appropriate victim-support, platform, financial, transport, or law-enforcement partners through lawful channels.
5. Preserve evidence and auditability.
6. Measure prevention and disruption outcomes without causing unauthorized surveillance, harassment, or re-traumatization.

KEEL is **not** a general morality-enforcement system, not a public accusation platform, and not a substitute for courts, law enforcement, or victim-service providers.

---

2. Mission and Objectives

Mission: Reduce the harm of sexual exploitation enterprises by giving authorized defenders a lawful, victim-centered, auditable system to detect patterns, coordinate disruption, and support prevention.

Objectives:

- Standardize intake and triage against the legal definition.
- Improve early detection of ongoing organization and patterns of exploitation.
- Support lawful evidence preservation and chain of custody.
- Coordinate prevention and disruption actions across approved partners.
- Protect victims and survivors from further harm.
- Maintain due process, privacy, and civil-liberties safeguards.
- Produce measurable outcomes: faster triage, validated disruptions, victim referrals, reduced false positives, and audit compliance.

---

3. Scope and Legal Definition

3.1 In Scope

KEEL applies to suspected **sexual exploitation enterprises** as defined in the source document, including entities or groups that engage in, facilitate, promote, or profit from a pattern of sexual exploitation.

KEEL shall classify matters against the following required elements:

1. **Entity or group** — individual, partnership, corporation, association, legal entity, union, or group associated in fact.

2. **Ongoing organization** — formal or informal shared purpose and continuity of structure or personnel.
3. **Pattern of exploitation** — non-consensual, coercive, or abusive use of another person's sexuality, intimacy, or bodily autonomy for financial gain, economic benefit, power, leverage, or commercial advantage.
4. **Included conduct** — sex trafficking; non-consensual production, distribution, syndication, commercialization, extortion, blackmail, or deepfake dissemination; operation or financing of abusive establishments or platforms; systemic abuse of authority or vulnerability.
5. **Commerce nexus** — actual or intended effect on interstate, foreign, or intrastate commerce, including electronic communications, financial networks, or transport systems.

3.2 Out of Scope

KEEL shall not be used for:

- Consensual adult activity.
- General morality policing.
- Unauthorized surveillance, hacking, doxxing, or public shaming.
- Direct physical intervention or vigilante action.
- Automated adverse action without human review, except approved emergency escalation.
- Unverified public accusations.
- Activities prohibited by applicable law or partner policy.

---

4. Guiding Principles

1. **Victim-centered and trauma-informed.** Victim safety and consent guide intake, referral, and communication.
2. **Lawful authority only.** KEEL operates under applicable law, MOUs, and platform/partner policies.
3. **Human review for consequential actions.** Automated systems flag and prioritize; humans validate and decide.
4. **Minimization and privacy.** Collect only what is necessary; retain only as long as required.
5. **Due process and false-positive control.** Association does not equal guilt; entity resolution must be reviewed.
6. **Security by design.** Least privilege, encryption, immutable audit logs, and role-based access.
7. **Transparency and oversight.** Independent review, appeal paths, and published metrics where safe.

8. **Do no harm.** Avoid re-identification, retaliation risk, and re-traumatization.

---

5. KEEL Leveling Model

“Leveled” means brought under lawful control, accountability, and disruption — not physical or violent action.

Level	Name	Meaning	Example System Response
0	Unaware	No report or indicator	Awareness and prevention content
1	Detected	Report or indicator received	Intake, triage, safety check
2	Validated	Human review confirms elements or high concern	Case opened, evidence preserved, partner review
3	Disrupted	Lawful disruption action taken	Platform referral, financial referral, LE referral, victim support
4	Deterred / Prevented	Harm reduced or enterprise deterred	Outcome recorded, monitoring, prevention follow-up

---

6. System Capabilities and Components

6.1 KEEL Intake Gateway

Receives reports from approved sources: victim/survivor referrals, NGO partners, platforms, financial institutions, transport partners, law enforcement referrals, and internal trust-and-safety teams. Includes safety screening and immediate-harm escalation.

6.2 Classification Engine

Maps intake data to the legal elements in Section 3. Produces a structured “element coverage” view. Does not make final legal conclusions. Requires human review before validation.

6.3 Entity Registry and Network Graph

Records suspected entities, aliases, associated persons/groups, infrastructure, financial indicators, and shared patterns. The graph supports analysis but must not infer guilt from association.

6.4 Pattern Detection and Risk Scoring

Identifies repeated conduct, continuity, shared infrastructure, commerce indicators, and victim-harm severity. Risk scores are advisory and must be explainable and auditable.

6.5 Case and Evidence Vault

Stores case records, evidence metadata, chain-of-custody logs, legal holds, and review decisions. Access is role-based and logged.

6.6 Action Orchestrator

Manages approved prevention and disruption playbooks: victim-support referral, platform takedown request, financial institution referral, transport referral, law-enforcement escalation, and internal monitoring. Consequential actions require human approval unless an approved emergency protocol applies.

6.7 Partner Portal

Provides scoped, audited access for approved partners. Partners see only minimum necessary information under MOU and data-sharing rules.

6.8 Victim Support Router

Connects victims/survivors to approved support services with consent, or under emergency protocol where legally required. Tracks referral completion without exposing unnecessary case details.

6.9 Oversight and Audit Console

Provides immutable logs, decision records, access reviews, appeals, and compliance reporting.

6.10 Reporting and Metrics

Produces operational and safety metrics with privacy thresholds and disaggregated false-positive and disparate-impact reporting.

---

7. Core Workflow

1. **Receive** — Report enters KEEL Intake Gateway.
2. **Safety screen** — Imminent harm? If yes, escalate under emergency protocol.
3. **Triage** — Categorize, remove duplicates, check jurisdiction and source authority.

4. **Element mapping** — Map facts to entity, ongoing organization, pattern, included conduct, and commerce nexus.
5. **Human validation** — Analyst and legal/policy reviewer assess confidence.
6. **Case decision** — Close with reason, monitor, enrich, or open validated case.
7. **Action selection** — Choose least-harm, lawful action: victim support, partner referral, platform referral, financial referral, LE referral, or prevention follow-up.
8. **Human approval** — Required for consequential actions.
9. **Execute and record** — Action logged with rationale and outcome.
10. **Review and appeal** — Periodic review, correction, and appeal path.
11. **Retention/disposal** — Apply retention schedule and legal holds.

---

8. Data, Evidence, and Retention Rules

- Collect minimum necessary data.
- Label sensitive data and restrict access.
- Maintain chain-of-custody for evidence.
- Do not ingest illegally obtained data.
- Do not use victim imagery beyond lawful, necessary review; use hashing and controlled access where possible.
- Separate suspicion from validated findings.
- Record confidence levels and reviewer identity.
- Apply retention schedules; preserve under legal hold when required.
- Delete or de-identify data when no longer needed.

---

9. Roles and Governance

Role	Responsibility
System Owner	Accountable for operation and policy compliance
Trust & Safety / Analysts	Triage, enrichment, validation support
Legal Counsel	Legal review, element interpretation, partner agreements
Victim Advocate	Safety planning, consent, referral quality
Security Team	Access control, incident response, audits
Data Protection Officer	Privacy impact assessments, retention, data subject requests

Partner Liaison	MOU coordination and scoped data sharing
Oversight Board	Independent review, appeals, policy updates

Governance requirements: written policies, training, access reviews, audit logs, incident response, appeals process, and independent review of high-impact actions.

---

10. Legal, Ethical, and Security Controls

- Lawful basis documented for each data source and action.
- Human review for validation, referral, and disruption.
- No unauthorized surveillance, hacking, or public disclosure.
- Minors: heightened safeguards and mandatory specialist review.
- Cross-border matters: jurisdiction check before action.
- Security: zero trust, MFA, RBAC, encryption in transit and at rest, immutable logs, vulnerability management, and incident response.
- Bias and false-positive testing before launch and periodically thereafter.
- Vendor and partner risk assessments.
- Whistleblower and retaliation protections.

---

11. Metrics and Success Criteria

Operational metrics: intake volume, time to triage, time to validation, case backlog, action completion, partner response time.
Safety metrics: victim-support referral completion, retaliation/safety incidents, re-traumatization reports, data-access violations.
Quality metrics: false-positive rate, validation precision, appeal outcomes, audit findings.
Prevention metrics: disrupted enterprises, removed abusive infrastructure, deterrence indicators, prevention content reach.
Guardrail metrics: disparate impact, unauthorized access, retention compliance.

---

12. Deployment and Acceptance Gates

Phase 1 — Design and legal review: DPIA, legal mapping, partner MOUs, security architecture.
Phase 2 — Controlled pilot: limited sources, human-heavy review, no automated consequential actions.

Phase 3 — Evaluation: false-positive thresholds, victim-safety review, security audit, oversight approval.
Phase 4 — Limited production: expanded partners and playbooks under audit.
Phase 5 — Scale: only after acceptance gates and independent review.

Pilot acceptance criteria: approved legal basis; completed DPIA; security audit passed; victim-support protocol approved; false-positive threshold met; audit logging verified; oversight board sign-off.

---

13. Key Risks and Mitigations

Risk	Mitigation
False accusations	Human validation, confidence labels, appeal path
Unauthorized surveillance	Legal review, source approval, access controls
Victim re-traumatization	Trauma-informed intake, consent, minimum data
Data breach	Encryption, RBAC, monitoring, incident response
Automation bias	Explainable scoring, mandatory human review
Mission creep	Scope limited to defined sexual exploitation enterprise elements
Partner misuse	MOUs, scoped access, audit, termination rights

---

Appendix A — Intake Checklist Mapped to Legal Elements

- □
  Entity/group identified?
- □
  Ongoing organization or continuity indicated?
- □
  Pattern of non-consensual, coercive, or abusive conduct indicated?
- □
  Included conduct category selected?
- □
  Financial gain, economic benefit, power, leverage, or commercial advantage indicated?

- □ Commerce nexus indicated: electronic systems, financial networks, or transport?
- □ Immediate-harm screen completed?
- □ Victim-safety and consent considerations recorded?
- □ Source lawfulness confirmed?
- □ Human reviewer assigned?

Appendix B — Action Matrix

Confidence / Severity	Default Action
Low confidence, no imminent harm	Monitor or close with reason
Medium confidence	Enrich, human review, victim-support routing
High confidence, validated elements	Open case, preserve evidence, partner referral
Imminent harm	Emergency escalation under approved protocol
Any consequential action	Human approval and audit log required

---

End of document.

Devin Mallonee
The Department of The Interior