

# ODNCA-POL-003 · Dispute & Abuse Policy

Warnings, blocks, signed flags – and the limits of all three

**Status:** v1.0 — Adopted

**Companion documents:** ODNCA-STD-001 (Resolution), ODNCA-STD-002 (Protocol Parameters Registry — thresholds and timers), ODNCA-POL-002 (Registrar Requirements).

## 1. What this policy can and cannot do

A name on the chain cannot be seized, edited, or deleted — not by ODNCA, not by anyone. **The indexer indexes everything, always**; the fact layer is neutral and stays neutral. What this policy governs is the **service layer**: whether the coordinated ecosystem's resolvers, browsers, mail, and tooling serve a name's content, serve it with a warning, or refuse to serve it.

Three consequences follow and bind everything below:

1. Enforcement here is *refusal of service*, never *removal of property*.
2. Every measure is per-operator: each resolver operator applies this framework under its own jurisdiction's law (for ORDnet: the Netherlands / EU) plus the universal categories in §4.1. A second, independent operator is therefore not a threat to this policy but its safety valve.
3. Honesty is absolute: a blocked name is *shown as blocked*. The ecosystem never pretends a name does not exist.

## 2. Statuses

| STATUS  | RESOLUTION          | CONTENT                                       | DISPLAY                                               |
|---------|---------------------|-----------------------------------------------|-------------------------------------------------------|
| ACTIVE  | normal              | loads                                         | normal                                                |
| WARNING | normal              | behind a pop-up; one click shows it           | warning disclosed, reason category shown              |
| BLOCKED | refused for content | replaced by the standard warning/offline page | explicit <code>blocked</code> answer with reason code |

A `blocked` answer is never disguised as `not_registered`. The name exists; the operator declines to serve it, and says so.

## 3. The flag system: the crowd can warn, only review can block

Anyone may report a name by **signing a flag transaction** — a report that costs a signature and a transaction. Flagging is thereby accountable and non-free: mass complaints carry mass cost and a paper trail.

The central design rule, adopted deliberately: **flags trigger the reversible tier automatically; the irreversible tier requires human review**.

1. At the flag threshold (a published parameter in ODNCA-STD-002, adjustable without revising this policy), the name automatically enters **WARNING** and moves to the top of the review queue.
2. An unjust automatic warning costs its target one click per visitor and is lifted the moment review clears it — cheap, reversible, safe to automate.
3. **No flag count ever causes a BLOCK**. Blocking is exclusively a review outcome (§5). Bought or coordinated flags therefore cannot take anyone offline; at most they buy the target a pop-up and an expedited inspection — and if the content is clean, the attack ends as a public clearance.

## 4. Triage: what gets blocked directly, what gets a chance to cure

The dividing line is not the number of reports but the **nature of the harm**: irreparable harm is closed immediately; reparable harm gets the chance to be repaired.

### 4.1 Direct BLOCK — no warning phase

Reserved for content where every second online creates victims and no modification can cure it:

- Child sexual abuse material (CSAM)
- Actively harmful malware or live phishing operations
- A binding order of a competent court

For these categories a warning phase would make the operator complicit; the block is applied on confirmation and the entry is published (§6).

### 4.2 Everything else — warning first, cure period, then review

Alleged IP infringement, suspected (unconfirmed) scams, shocking-but-not-evidently-illegal content, disputes over a name or its content:

1. **WARNING** is applied and the holder is notified with the reason.
2. A **cure period** (default 7 days; a published parameter) allows the holder to modify the content.

3. After the period, **review** decides: clear (back to ACTIVE), warning stands, or escalate to BLOCKED.

IP-infringement blocks based on contested ownership follow only a competent court's ruling, never the operator's own judgment of who is right.

---

## 5. Review

Review is human, documented, and its outcomes are published. Every review answers: which category (§4.1 or §4.2), which evidence, which outcome, effective when. Reviews triggered by flags additionally record the flag count and note whether coordinated flagging was suspected — abuse of the flag system is itself publishable conduct.

---

## 6. The public blocklist

Blocking in secret is censorship; blocking in public is moderation anyone can recompute. Every operator publishes its list:

- **Versioned and dated** — every addition and removal is a dated changelog entry.
  - **Reasoned** — every entry carries a reason code (category from §4) and effective date.
  - **Signed** — the list is signed with the operator's resolver key (the same key infrastructure as ODNCA-STD-001 §7), so tampering and silent edits are detectable.
- 

## 7. Appeal

A holder may appeal any WARNING or BLOCK to the operator that applied it. Appeals are reviewed by someone other than the original reviewer where feasible, answered within the published response window, and their outcomes are published. The chain-level escape is acknowledged rather than denied: a holder who disagrees may seek service from another operator, and the transparency of §6 is exactly what makes that choice an informed one.

---

ODNCA — the ORDnet Decentralized Names Coordination Authority. Don't trust us — recompute us.