(D40) TCORF Non-Compliance Handling Protocols

Standard Operating Procedures for Remediation Requests

Referenced by: D31 TCORF Framework (Rights Catalogue)

Contents

1. Purpose (What this document is)

This document defines a standardized request and documentation process for Owners (Citizens) who want to report and challenge a violation of a TCORF Right (D31).

TCORF is not a court and does not enforce outcomes.

TCORF provides a repeatable format for:

- describing violations clearly,
- attaching objective evidence,
- requesting standardized remedies,
- and enabling cumulative signals at scale (“agreement in advance without coordination”).

The purpose is awareness, traceability, and pressure through comparability, even if enforcement is absent.

2. Operational Disclaimer

This document provides standardized request procedures for documentation and governance QA. It is not legal advice, not a guarantee of enforceability, and not a replacement for courts, police, or emergency services. Users are solely responsible for assessing operational risk, including the risk of retaliation, aggressive non-compliance, or legal exposure resulting from public publication. In high-risk environments, users should begin with a Silent Educational Phase (“Shadow Audit”) before initiating any contact or public filing. Refer to Document 53 (Disclaimer [REF:D53]) and Document 51 (Terms of Use [REF:D51]) before deployment.

3. Active Mode + Real-World Interaction

Active Mode claims under TCORF must maintain a **clear distinction between procedural tooling and source of authority.**

TCORF does not constitute a legal system, nor does it independently confer enforceable rights. Accordingly, an Active Mode claim **must not assert entitlement on the basis that a TCORF-defined right has been violated**, unless such a right is independently recognized by the external system involved.

All Active Mode claims must instead be framed around externally grounded interests, including but not limited to:

- Ownership, custodial, or stakeholder interests
- Legal, contractual, regulatory, or policy-based obligations
- Civic or administrative duties with identifiable impact
- Procedural failures producing tangible harm or risk

The TCORF Framework functions as a neutral procedural interface that allows such issues to be:

- Formally documented
- Transparently communicated
- Tracked through defined resolution paths

This requirement preserves the legitimacy, accuracy, and interoperability of TCORF-based claims and prevents mischaracterization of TCORF as a source of binding authority.

4. Key Definitions

- Owner / Citizen (Owner): a member of the co-owned organization who may file a request.
- Organization: the co-owned entity and its offices.
- Agent: any employee, contractor, delegated person, office-holder (elected or appointed), or outsourced actor acting for the organization.
- Request: a written demand for remediation of a specific TCORF Right violation under this SOP.

5. Who May File

A. Default rule

Only individual Owners may file requests (no coordination required).

B. Filing on behalf of others (exception)

An Owner may file on behalf of another person only in special cases where that person is unable to file (e.g., missing, unlawfully detained, dead, permanently unconscious).

6. Owner Chooses the Submission Method (Digital is optional)

If a complaint portal or platform exists, the Owner is not required to use it.

Reasons:

- the Owner may be cut off (no internet, hardware, software, ID, transport),
- digital systems can be inaccessible or restrictive,
- digital systems can fail or become selectively unavailable.

Paper submission is always valid.

TCORF treats paper trail as a protected option, not an exception.

7. Minimum Required Intake Availability

Every organization must provide at least:

One postal intake address (reachable by mail) for TCORF requests.

If no official complaint postal address exists, is not well-known, or is not accessible, intake must be possible via any reachable public-facing point of contact, including but not limited to:

- a local authority office,
- police station,
- post office,
- school administration,

- any official front desk capable of forwarding internally.

“No intake point exists” is not acceptable.

8. Mandatory Intake Rule (No “Wrong Office” Defense)

An organization may claim it is not the responsible processing office. This is not a valid reason to reject intake.

Minimum required behavior:

1. Accept intake (paper or digital).
2. Issue a receipt / request number (proof of registration).
3. Forward internally to the responsible unit without delay.
4. Preserve the request content (no deletion, alteration, hiding, “lost in transit”).

Rejecting intake, refusing registration, or refusing a receipt is Process Obstruction and may be treated as a separate non-compliance event.

9. Manual Intake Mode (Always Available Fallback)

Manual Intake Mode exists to ensure that requests can always be filed, even when:

- no valid/well-known complaint postal address exists

In Manual Intake Mode, the receiving office must:

1. Accept the request immediately (paper or any available channel).
2. Issue a manual receipt containing:
   - date/time,
   - receiving office/location,
   - signature or stamp where possible,
   - and a temporary reference number (or written acknowledgment).
3. Forward internally to the responsible unit without delay.
4. Register later when possible, without altering the content.

Manual mode is a protected baseline.

It is not optional, and it is not a “downtime exception.”

10. Request Handling Capacity Is Not a Defense

Organizations may claim they cannot process requests due to lack of staff, budget, software, or capacity.

TCORF rejects “capacity” as a defense for unprocessed core-rights violations.

Owners have the right to a rapid, standardized request procedure for core rights.

If violations exist, it is the organization’s responsibility to scale intake and processing to match real demand.

If the organization cannot process high volumes, that indicates the organization lacks a functioning complaint and QA capability — which is itself a governance failure.

TCORF supports scalability through:

- strict request formatting,
- one-violation-per-request structure,
- and bundling of materially identical requests.

11. How to Write a Request (Objective Evidence Standard)

A valid request must meet these minimum standards:

- Max 500 words
- One request = one specific Right violation (one case)
- Must include:
    1. Right number + Right title (from D31)
    2. What happened (facts only)
    3. Where/when (dates, times, locations)
    4. Which office / role (as precisely as possible)
    5. Evidence attached or referenced (documents, videos, photos, witness names, timestamps)
    6. Requested outcomes (from the Outcome Menu below)

Evidence may be attached without additional text.

The request body must remain short, auditable, and focused.

12. Acknowledgment Targets (Receipts)

Organizations must acknowledge and register requests as follows:

- Digital acknowledgment target: within 48 hours (where available)
- Manual / postal acknowledgment target: within 168 hours (7 days)

For manual/postal requests, acknowledgment deadlines start when the request is received by any valid intake point (including fallback locations described in Sections 6 and 8).

Refusal to acknowledge, register, forward, or issue a receipt may qualify as Process Obstruction, especially when repeated.

13. Timestamp of Notice (Owner-controlled proof)

After dispatching a request, the Owner does not have to wait for confirmation.

The Owner may immediately document and/or publicize the filing as their Timestamp of Notice, using proof such as:

- postal proof of delivery / registered mail,
- photos/video of submission,
- witness confirmation,
- email records,
- portal submission confirmation,
- or any comparable evidence.

Safety note: publicizing can provide protection through visibility in some environments and increase risk in others. The Owner decides what is safe.

14. Bundling Rules (Batch Processing)

Bundling is allowed to reduce processing cost when many requests are materially identical.

Bundling requirements:

- No information loss: every underlying request must remain accessible.
- Material identity: same Right, same violation pattern, same requested outcomes, and the same relevant roles/offices (as applicable).
- QA threshold: bundling allowed only if error rate stays below 1%.
- If error rate exceeds 1%, bundling is suspended for 1 month.

Bundling is a scalability tool, not a way to erase details.

15. Outcome Menu, A1-A3, B1-B2, C1-C3, D1-D2 (Standardized Administrative Requests)

These are HR / operational outcomes, not criminal sentencing.

They are written as standardized options so many Owners can independently request the same thing without coordination.

A) Stop / Correct / Undo

- A1 — Cessation: stop an active violation immediately
- A2 — Correction: provide missing information, restore access, redo a defective process
- A3 — Annulment request: treat a specific action/procedure as invalid because of non-compliance

B) Termination Requests (HR)

- B1 — Termination with severance (standard payout / contractual minimum)
- B2 — Termination without severance (breach of trust, process obstruction, severe abuse cases)

C) Employment / Mandate Exclusion (Eligibility Restriction)

- C1 — 4-year exclusion (default serious non-compliance / process obstruction deterrence)
- C2 — 10-year exclusion (high severity rights)
- C3 — Lifetime exclusion (extreme rights violations such as persecution, forced labor, camps, murder)

D) Financial Accountability

- D1 — Restitution to the victim/Owner
- D2 — Clawback / reimbursement of unauthorized gains or spending

E) Cooling-Off Period Without Immunity

A standardized request that a leader must serve a continuous period without immunity, as specified by the relevant Right in D31.

16. Accountability Attachment Rule (Minimum Chain)

For any request that alleges a violation or Process Obstruction, the Organization must attach administrative accountability review to **at least three roles** where applicable:

1. **Primary actor** (the Agent who executed the action)
2. **Direct supervisor** (line manager responsible for oversight)
3. **Department head / unit head** (senior responsible leader)

Organization's failure to identify and route potential accountability to the required chain may qualify as **Process Obstruction**.

17. Processing Targets (Service Level Targets for Audit)

Deadlines are targets used for audit, comparability, and accountability:

- Emergency (life/liberty threat): 48 hours
- Current issues: 30 days
- Past 12 months: 45 days
- Past 4 years: 90 days
- Past 5–25 years: 180 days

If a Right defines specific deadlines or protocols, those override D40's general service targets.

18. Process Obstruction Clause

Process Obstruction includes: refusing intake, refusing registration/receipt, refusing internal routing, altering/hiding requests, or retaliating against the requester.

Any Agent who:

- refuses intake,
- refuses registration or receipt,
- refuses forwarding/routing internally,
- hides, alters, deletes, or misroutes requests,
- delays without justification,
- retaliates against a requester,

creates a separate non-compliance event: Process Obstruction.

Owners may file a separate request specifically about obstruction, because a system that cannot receive and process requests is itself non-compliant.

19. Transparency & Logs (Desirable Implementation — Safety First)

TCORF supports tracking through logs to identify patterns.

Request Log ("Shadow Log") — recommended

A log of requests with long retention helps identify repeated patterns and support audits.

Publication — optional and context-dependent

In stable environments, publication increases accountability.

In high-risk environments, publication can increase danger.

Any publication system should support:

- delayed publication,
- anonymization,
- role/office-based identification when possible,
- private escrow storage,
- and export access for independent analysis.

Exclusion lists — optional and environment-dependent

Eligibility lists can prevent rehiring of excluded individuals in stable environments.

In unstable environments, they may increase risk and misuse.

TCORF therefore treats eligibility lists as optional, not mandatory.

20. Integrity Rule (False Accusations and Misuse)

TCORF is designed for good-faith, evidence-backed requests.

Knowingly false claims, harassment, or abuse of the process:

- damages the credibility of the framework,
- may expose the requester to legal and operational risk,
- and undermines the purpose of standardized oversight.

Owners should publish carefully and stick to objective evidence.

21. Ticketing Principle (Why this is a system)

Each request is a trackable incident.

The organization’s inability to process incidents at volume is not the citizen’s burden.

It is an organizational failure that must be corrected.