

DATA GOVERNANCE & CONTAMINATION PLAN — MENS-SCCA × APEX

Data boundaries, provenance, contamination control, and publication

1. PURPOSE

Define access, provenance, exposure, transformation, use, and publication boundaries before confirmatory execution.

2. FOUR-ZONE SEPARATION

Zone A — MERCOR CONFIDENTIAL: reserved tasks, data, environments, executions, rubrics, or materials designated confidential/restricted.

Zone B — EXPERT / REFERENCE: expert rubrics, annotations, professional criteria, and reference materials.

Zone C — MENS-SCCA INFRASTRUCTURE: research code, specifications, documentation, fixtures, and methodological components owned or controlled by the researcher.

Zone D — AUTHORIZED DERIVATIVES: aggregate tables, metrics, results, fixtures, or artifacts whose extraction/publication is explicitly authorized.

3. PRIMARY DATA RULE

Mercor primary data remain in authorized environments. Public repositories will not contain reserved tasks, confidential documents, credentials, unnecessary personal information, proprietary content, or trajectories that permit reconstruction of protected materials.

4. PROVENANCE

Where possible, each relevant artifact should carry: `artifact_id`, `source_class`, `creation_date`, `access_group`, `task_id`, `run_id`, `benchmark_split`, `training_exposure`, `publication_status`, `license_status`, and `transformation_history`.

The objective is a sufficient provenance chain to reconstruct where an observation came from and what transformations it received.

5. CONTAMINATION CONTROL

DEVELOPMENT — permitted for design/calibration.

PILOT — permitted for testing.

HELDOUT — reserved for confirmatory evaluation.

RESTRICTED — not usable without specific authorization.

Held-out tasks will not be used retrospectively to tune confirmatory instruments, rubrics, or hypotheses.

6. TRAINING EXPOSURE

When information is available, exposure of models, agents, judges, or evaluation components to tasks, documentation, or derivatives will be recorded. Lack of evidence will not be treated as proof of non-exposure; it will be recorded as unknown when appropriate.

7. DEVELOPMENT VS. CONFIRMATION

DEV/PILOT may adjust instrumentation format, fixtures, ingestion procedures, rubric clarity, and technical error handling.

Before confirmation, hypotheses, primary variables, partitions, success criteria, statistical plan, exclusion procedures, and instrument/rubric versions must be fixed. Later changes that affect confirmatory hypotheses are treated as exploratory and versioned.

8. ACCESS AND MINIMUM NECESSITY

Access will be limited to what is necessary for the authorized research task. The preferred pattern is authorized environment → minimal extraction → instrumentation → metrics → analysis → authorized derivative.

9. PUBLICATION

Artifacts will be classified as PUBLICABLE, PUBLICABLE WITH TRANSFORMATION, or CONFIDENTIAL / NOT PUBLICABLE.

Public outputs should favor aggregates, synthetic examples, researcher-owned fixtures, and methodological documentation when those forms support reproducibility without exposing protected materials.

10. CODE AND LICENSING

An eventual public package may contain only researcher-owned or appropriately licensed code, authorized fixtures, documentation, schemas, synthetic/derived data, and reproducible instructions.

11. GOVERNANCE PRINCIPLE

The existence of an artifact in the research environment does not by itself establish permission to publish, redistribute, train on, or disclose it. Authorization status remains explicit and versioned.