ZAKON PI2 — Deploy Verification Protocol

ZAKON PI2 — Deploy Verification Protocol (enforced)

Status: ACTIVE — 2026-04-22 **Origin:** ALAI incident 2026-04-22 (Bilko demo fix deployed to wrong branch, Intesa content leaking on public URL, CI broken for 7 days undetected) **Owner:** pi-orchestrator v2 **Violation penalty:** task auto-blocked, re-work required, logged to MC

Why This Exists

On 2026-04-22 a 3-bug Bilko fix sprint ran for 2 hours and produced **zero live changes** because:

- Wrong branch inferred from memory (no `curl` + `git log` verification)
- CI pipeline silently broken for 7 days (no health check)
- `--no-traffic` flag blocked all past deploys (never verified)
- Intesa pitch content leaking to public demo (no branch-purity check)
- PAT missing `workflow` scope (no auth audit)
- MC tasks marked `ready_for_review` without live verification

All these are preventable with **6 hard checks**. This ZAKON makes them mandatory.

The 7 Hard Checks (every deploy task)

Check 0 — Mehanik Clearance (NEW — 2026-04-25, MC #9223 root-cause)

Before any deploy preflight check (curl, git log, gh run list) — verify Mehanik gate clearance:

```
MC_ID={your_task_id}
MARKER="/tmp/mehanik-cleared-$MC_ID"

if [[ ! -f "$MARKER" ]]; then
  echo "BLOCKED: No Mehanik clearance for MC #$MC_ID. Run /mehanik first."
  exit 2
fi

MARKER_AGE=$(( $(date +%s) - $(stat -f %m "$MARKER") ))
if [[ $MARKER_AGE -gt 14400 ]]; then
  echo "BLOCKED: Mehanik clearance for MC #$MC_ID is stale (>4h). Re-run /mehanik."
  exit 2
fi
```

If Check 0 fails → STOP. Do not proceed to Check 1 (curl preflight). Run `/mehanik` to obtain clearance, then retry.

Rationale: Per /tmp/9223-final-synthesis.md (sentinel-architect), deploy preflight at end-of-pipeline is too late. Pattern completion / scope creep happens BEFORE preflight runs. Mehanik gate at start = deterministic enforcement against hallucinated infra.

Check 1 — DEPLOY MAP must exist

Every repo that deploys MUST have `DEPLOY-MAP.md` at root:

```
| Branch | Service | URL | Workflow | Last verified |
|--------|---------|-----|----------|---------------|
| main   | bilko-web | bilko-demo.alai.no | gcp-deploy.yml | 2026-04-22 |
```

If missing: task blocks. Agent creates `DEPLOY-MAP.md` before any code change.

Check 2 — Pre-Flight Discovery (4 commands, no exceptions)

Agent must run and paste output into MC task BEFORE touching code:

```
curl -sI <target-url> | head -3
git log <target-branch> --oneline -5
gh run list --repo <owner/repo> --branch <target-branch> --limit 3
gcloud run services describe <service> --region <region> --
```

```
format='value(status.latestReadyRevisionName,status.url)'
```

If any returns unexpected: STOP, escalate to John. Do not proceed.

Check 3 — Branch Purity Gate (CI)

Every repo gets `.github/workflows/branch-purity.yml`:

```
find apps/web/app -type d \( -name "intesa-*" -o -name "corpint-*" -o -name "lumiscare-*" -o -name "<client>-*" \) | grep . && exit 1 || exit 0
```

Client-specific routes MUST live on dedicated branch + dedicated service. Never on main.
Registry: `~/system/rules/client-prefix-registry.md` lists all reserved prefixes.

Check 4 — CI Health Pre-Check

Before any push to a deploy branch:

```
gh run list --repo <owner/repo> --branch <branch> --limit 5 --json status,conclusion
```

If last 5 runs all `failure` → CI is broken → fix CI first OR use documented manual deploy path (written in `DEPLOY-MAP.md`). **No push on broken pipeline.**

Check 5 — Post-Deploy Evidence Gate

MC task CANNOT move to `done` without ALL three:

1. `curl -sI <URL>` returning 200 (paste in task notes)
2. Playwright CLI screenshot saved to `docs/evidence/<task-id>/`
3. `gcloud run revisions list` showing NEW revision serving 100% traffic

`mc.js done` without evidence = blocked automatically.

Check 6 — Auth Scope Audit (session start)

`bash ~/system/boot.sh` runs:

```
gh auth status --show-token 2>&1 | grep -E "Token scopes|Logged in"
gcloud auth list --format='value(account,status)'
```

If missing `workflow` scope OR gcloud expired → BLOCKER logged to MC, Alem notified before any deploy task dispatched.

Enforcement

Level 1 — Agent self-enforcement

Every pi2-dispatched agent includes this rule in its system prompt. Agent refuses to proceed if any check fails.

Level 2 — Hook enforcement

`~/.claude/hooks/pre-deploy-check.sh`:

- Triggers on `gcloud run deploy`, `git push origin main` from repos with `DEPLOY-MAP.md`
- Runs Check 2 + Check 4
- Exits non-zero if fails
- Output logged to MC

Level 3 — MC auto-block

`mc.js done <id>` for tasks with `category: deploy|frontend|backend|devops` AND `priority: H` requires:

- Evidence JSON at `docs/evidence/<task-id>/verification.json`
- Without it: reverts to `ready_for_review`

Client Prefix Registry (Check 3 reference)

Prefixes that MUST NOT appear on main:

- `intesa-*` → Intesa Sanpaolo pitch (feat/intesa-bih-demo → bilko-intesa-demo Cloud Run)
- `corpint-*` → Corpint deal specific
- `lumiscare-*` → LumisCare product routes
- `drop-*` (Bilko/Tok repos only, not Drop's own)
- `tok-*` (Bilko/Drop repos only)

Add new entries here when client-specific branches spawn.

How to Apply

When a task says "fix demo" / "deploy X" / "push fix":

1. Open `DEPLOY-MAP.md` — confirm branch/service/URL
2. Run 4 pre-flight commands — paste output in MC task
3. Verify CI health — if red, STOP
4. Make change, push
5. Run post-deploy evidence gate — 3 artifacts
6. Only then: `mc.js done`

If any check returns unexpected: do not invent a workaround. Report to John.

Escape Hatch

Single emergency override: CEO-only command `mc.js done <id> --force --ceo-override "<reason>"` bypasses Checks 1-5. Logged to audit, reviewed weekly by John.

Change Log

- 2026-04-25 — Check 0 added (MC #9223 root-cause). Mehanik clearance now required before deploy preflight.
- 2026-04-22 — Initial ZAKON PI2 created after Bilko demo deploy incident.

Related Rules

- `~/system/rules/claim-verification-protocol.md` — broader no-claim-without-evidence
- `~/system/rules/closed-loop-build.md` — build-test-verify loop
- `~/system/rules/john-operating-system.md` — John's decision tree
- `~/.claude/projects/-Users-makinja/memory/feedback_verify_deploy_target_before_code.md` — incident source

Revision #3
Created 2026-04-30 19:25:02 UTC by John
Updated 2026-06-22 02:52:28 UTC by John