**MCPX‑KendoBridge — CODEOWNERS Policy & File**

**Document:** .github/CODEOWNERS.docx  
**Project Code:** MCPX‑KendoBridge  
**Version:** 2.0.0  
**Last Updated:** 2025‑09‑27  
**Owner:** DoSE (Accountable) — DocFactory (Author/Responsible) — SRE/QA/SecLead/DBA/T‑Arch/UI Leads (Consulted)

**Purpose.** Define repository **ownership and review routing** that enforces Technijian’s **GitHub‑first** SDLC, merge‑queue‑based reviews, and required checks across **Alpha → Beta → RTM → Prod** promotions. CODEOWNERS ensures the right people review changes that affect the API transport, streaming behavior, DB contracts, CI/CD workflows, and evidence gates.

**Compliance banners (always in effect):**

* **Add‑only** schema evolution; **Stored‑procedure‑only** DB access with **EXECUTE‑only** grants.
* **No‑Hard‑Coding** of dynamic values (child command/args/cwd, timeouts/keep‑alive, Origin allow‑list, feature flags) — all sourced from SQL via sp\_Config\_\*, sp\_Feature\_IsEnabled, sp\_Lookup\_Get.
* **Secrets** (SQL connection strings, Telerik license) live **only** in GitHub Environments and must **never** appear in code, DB, docs, or logs. CODEOWNERS complements branch protection to enforce these controls.

**1) Scope & Outcomes**

**Scope:** Entire MCPX‑KendoBridge repository, including API (.NET 8), DB migrations/SPs, KendoReact Admin Portal (read‑only), CI/CD workflows, runbooks, and documentation.  
**Outcomes:**

1. Every change is reviewed by **domain owners** before it enters the merge queue.
2. High‑risk paths (workflows, DB contracts, OpenAPI, compliance docs) always involve **Security** and/or **SRE/DBA** approvers.
3. Promotion through **Alpha → Beta → RTM (Prod DB read‑only) → Prod** is guarded by CODEOWNERS + required checks.

**2) Teams & Handles (replace with your org/team slugs)**

**Update these to match your GitHub org.** Examples assume @technijian/\* teams.

* **DoSE (Accountable)** — @technijian/dose
* **SRE Leads** — @technijian/sre-leads
* **Security (SecLead)** — @technijian/security
* **DBA** — @technijian/dbas
* **API Owners (.NET / Transport)** — @technijian/api-owners
* **UI Owners (KendoReact)** — @technijian/ui-owners
* **CI/CD Owners** — @technijian/cicd-owners
* **DocFactory (Docs/Runbooks/Evidence)** — @technijian/docfactory

**3) How CODEOWNERS interacts with branch protection**

* **Require review from Code Owners** must be **ON** for protected branches (e.g., main).
* Set **minimum approvals** (e.g., 2) and ensure the merge queue requires **all checks** (Build/Tests, **OpenAPI lint/diff**, **CodeQL**, **Dependency Review**, **Secret Scanning**, **SBOM**) before enqueue.
* CODEOWNERS **routes review**, while branch protection **enforces** approvals and checks.

**Note:** CODEOWNERS matches are order‑sensitive; **last match wins**. Avoid negations; prefer specific patterns above general ones.

**4) Ownership Matrix (review routing)**

| **Repo Area** | **Path Pattern(s)** | **Required Owners (at least one from each line)** |
| --- | --- | --- |
| **OpenAPI & Transport** | api/openapi/\*\*, api/openapi/mcp-proxy.yaml, api/\*\* | @technijian/api-owners + @technijian/security |
| **API (.NET 8)** | api/\*\*, src/\*\* (if API source lives here) | @technijian/api-owners |
| **Streaming/Transport Samples & Tests** | tests/\*\*, tests/gherkin/\*\* | @technijian/api-owners + @technijian/qa-leads |
| **DB Migrations & SPs** | db/migrations/\*\*, db/stored\_procedures/\*\* | @technijian/dbas + @technijian/security |
| **Admin Portal (KendoReact)** | web/\*\* | @technijian/ui-owners |
| **Workflows & CI/CD** | .github/workflows/\*\*, /.github/\*\* | @technijian/cicd-owners + @technijian/security + @technijian/sre-leads |
| **Docs & Runbooks** | docs/\*\*, runbooks/\*\* | @technijian/docfactory + @technijian/dose |
| **Security, Compliance & Threat Model** | docs/\*compliance\*, docs/\*threat\*, docs/error\_catalog.docx | @technijian/security + @technijian/dose |
| **Global Fallback** | \* | @technijian/dose |

These routes align with our **GitHub‑first** gates and ensure audits capture owner reviews for critical surfaces (OpenAPI, DB contracts, CI/CD, security docs).

**5) Drop‑in CODEOWNERS (plaintext file)**

**Place this exact block in**: .github/CODEOWNERS  
*(Replace @technijian/... with your real team slugs.)*

# ---------- MCPX-KendoBridge CODEOWNERS ----------

# Order matters; last match wins. Keep specific rules above generic ones.

# 1) OpenAPI & transport (must involve API + Security)

api/openapi/mcp-proxy.yaml @technijian/api-owners @technijian/security

api/openapi/\*\* @technijian/api-owners @technijian/security

# 2) API (.NET 8) implementation

api/\*\* @technijian/api-owners

# 3) Tests (E2E/contract/perf)

tests/gherkin/\*\* @technijian/api-owners @technijian/qa-leads

tests/\*\* @technijian/api-owners @technijian/qa-leads

# 4) Database (add-only migrations; SP-only)

db/migrations/\*\* @technijian/dbas @technijian/security

db/stored\_procedures/\*\* @technijian/dbas @technijian/security

# 5) Admin Portal (KendoReact, read-only)

web/\*\* @technijian/ui-owners

# 6) CI/CD workflows & repo policies

.github/workflows/\*\* @technijian/cicd-owners @technijian/security @technijian/sre-leads

.github/\*\* @technijian/cicd-owners @technijian/security

# 7) Docs & Runbooks (audit/Evidence)

docs/\*\* @technijian/docfactory @technijian/dose

runbooks/\*\* @technijian/docfactory @technijian/dose

# 8) Security, Compliance, Threat Model

docs/\*compliance\* @technijian/security @technijian/dose

docs/\*threat\* @technijian/security @technijian/dose

docs/error\_catalog.docx @technijian/security @technijian/dose

# 9) Fallback (anything else)

\* @technijian/dose

**Why these paths?** They map directly to our evidence‑bearing artifacts and controls (OpenAPI, CI/CD, Monitoring/SLOs, DB contracts), reinforcing the **No‑Hard‑Coding**, **SP‑only**, and **add‑only** guarantees across the repo.

**6) Required checks to pair with CODEOWNERS**

Enable these **branch protection** checks so CODEOWNERS routing results in enforceable gates:

* Build & Tests (.NET + UI, where applicable)
* **OpenAPI lint/diff** (fail on breaking changes)
* **CodeQL** (C#/JS)
* **Dependency Review** (fail on **High/Critical**)
* **Secret Scanning** (repo/org setting)
* **SBOM** artifact generation
* **Merge queue** with “Require review from Code Owners.”  
  These checks and the promotion flow are part of the standard DocFactory SDLC.

**7) Maintenance rules**

1. **Keep specific patterns above general ones**; last match wins.
2. **Update team slugs** when org team names change; test on a draft PR.
3. **Add new code areas** (e.g., new service folders) before landing their first large PR.
4. **Audit quarterly**: open a doc task to re‑confirm owners and branch‑protection settings; attach the checklist to the Evidence Pack.

**8) Risks & mitigations**

| **Risk** | **Impact** | **Mitigation** |
| --- | --- | --- |
| Stale team slugs | PRs bypass intended owners | Quarterly CODEOWNERS audit; small PR to update slugs |
| Over‑broad fallback (\*) | Excess load on DoSE | Keep specific rules comprehensive; route to domain owners first |
| Missing Security review on workflows or DB | Compliance gaps | Keep .github/\*\* and db/\*\* mapped to Security & SRE/DBA owners |
| Negations/overlaps cause confusion | Incorrect routing | Avoid negations; keep order clear; test on a sample PR |

**9) Acceptance checklist**

* .github/CODEOWNERS committed and visible in default branch.
* Branch protection: **Require review from Code Owners** enabled; **min 2 approvals** set.
* Required checks match the CI/CD plan (Build/Tests, **OpenAPI lint/diff**, **CodeQL**, **Dependency Review**, **Secret Scanning**, **SBOM**).
* Owners tested with a dry‑run PR touching each critical path (OpenAPI, db/\*\*, .github/workflows/\*\*, docs/\*\*).
* Evidence: screenshot of branch protection + CODEOWNERS file attached to the release (retention ≥ 1 year).

**10) Assumptions**

1. The repository is governed by the **GitHub‑first** SDLC with merge queue and environment promotions **Alpha → Beta → RTM (Prod DB read‑only) → Prod**.
2. **No‑Hard‑Coding**, **SP‑only**, and **add‑only** DB policies apply universally; CODEOWNERS helps enforce review by DBAs/Security where relevant.

**11) Next steps**

* Commit the **plaintext CODEOWNERS** file above into .github/CODEOWNERS.
* Verify branch protection and merge queue settings match §6.
* Create a **recurring issue** (quarterly) to review owners and branch policies; include it in the Evidence Pack.

**Footer (optional for Word header/footer):**  
*MCPX‑KendoBridge • CODEOWNERS Policy • v2.0.0 • 2025‑09‑27 • Confidential — Technijian Internal*

# ---------- MCPX-KendoBridge CODEOWNERS ----------

# Order matters; last match wins. Keep specific rules above generic ones.

# 1) OpenAPI & transport (must involve API + Security)

api/openapi/mcp-proxy.yaml @technijian/api-owners @technijian/security

api/openapi/\*\* @technijian/api-owners @technijian/security

# 2) API (.NET 8) implementation

api/\*\* @technijian/api-owners

# 3) Tests (E2E/contract/perf)

tests/gherkin/\*\* @technijian/api-owners @technijian/qa-leads

tests/\*\* @technijian/api-owners @technijian/qa-leads

# 4) Database (add-only migrations; SP-only)

db/migrations/\*\* @technijian/dbas @technijian/security

db/stored\_procedures/\*\* @technijian/dbas @technijian/security

# 5) Admin Portal (KendoReact, read-only)

web/\*\* @technijian/ui-owners

# 6) CI/CD workflows & repo policies

.github/workflows/\*\* @technijian/cicd-owners @technijian/security @technijian/sre-leads

.github/\*\* @technijian/cicd-owners @technijian/security

# 7) Docs & Runbooks (audit/Evidence)

docs/\*\* @technijian/docfactory @technijian/dose

runbooks/\*\* @technijian/docfactory @technijian/dose

# 8) Security, Compliance, Threat Model

docs/\*compliance\* @technijian/security @technijian/dose

docs/\*threat\* @technijian/security @technijian/dose

docs/error\_catalog.docx @technijian/security @technijian/dose

# 9) Fallback (anything else)

\* @technijian/dose