**MCPX‑KendoBridge — Pull Request Template**

**Document:** .github/pull\_request\_template.docx  
**Version:** 2.0.0  
**Last Updated:** 2025‑09‑27  
**Owner:** DoSE (Accountable) — DocFactory (Author/Responsible) — SRE/QA/SecLead/DBA/T‑Arch (Consulted)

**Compliance banners (must hold for every PR)**  
**No‑Hard‑Coding** of dynamic values. **Stored‑procedure‑only** data access with **EXECUTE‑only** grants. **Add‑only** DB migrations. **Secrets** (SQL connection strings, Telerik license) live **only** in GitHub Environments; never in code/DB/logs/evidence. **SSE** pass‑through (no ingress buffering) and **sticky routing** by Mcp‑Session‑Id preserved.

**1) Summary**

* **Title:**
* **Short description (what & why):**
* **Linked issue(s):** Fixes #… / Relates to #…
* **Change type (choose one):** Feature / Fix / Refactor / Docs‑Only / CI/CD / DB‑Only (add‑only) / Security / Performance

**2) Risk, Impact & Rollback**

* **User‑visible impact:** ☐ None ☐ Admin‑only UI ☐ API behavior (documented in OpenAPI)
* **Operational impact:** ☐ None ☐ Ingress/SSE config ☐ HPA/PDB ☐ Observability
* **Rollback plan:** link to **Rollback Runbook** steps and LKG image/tag.
* **Blast radius if rollback fails:** brief notes; mitigation.

**3) Scope of Changes (tick all that apply)**

* **API / Transport:** ☐ /mcp JSON ☐ /mcp SSE ☐ /mcp notifications (GET) ☐ Legacy (/messages//sse)
* **UI:** ☐ KendoReact (read‑only) ☐ Theme updates (ThemeBuilder) ☐ A11y
* **DB:** ☐ Migrations (add‑only) ☐ Stored procedures ☐ Grants/Roles
* **CI/CD:** ☐ Workflows ☐ CodeQL ☐ Dependency Review ☐ SBOM ☐ Evidence hooks
* **Monitoring:** ☐ Metrics/alerts ☐ Dashboards ☐ Synthetic probes

**4) Architecture & Compliance Checklist (required)**

**Guardrails**

* **No‑Hard‑Coding.** All runtime values come from **AppConfig/FeatureFlag/Lookup** SPs; no literals for child cmd/args/cwd, timeouts/keep‑alive, origins, flags.
* **SP‑only** DAL; app principal has **EXECUTE‑only** grants; **no table CRUD** rights.
* **Add‑only** DB migration strategy; no destructive DDL.
* **Secrets** absent from code, migrations, logs, UI; only in **GitHub Environments** (SQL, Telerik).
* **SSE** pass‑through intact (ingress **not buffering**); **sticky routing** by Mcp‑Session‑Id maintained.
* **Error envelope** { code, message, requestId? } used for all non‑2xx paths; updated **Error Catalog** if a new code is introduced.

**OpenAPI governance**

* api/openapi/mcp-proxy.yaml updated for any new/changed endpoint/headers/errors.
* Redocly **lint** clean; **diff** against the last tag reviewed and attached to Evidence.

**Environments**

* Alpha → Beta → RTM (validates on **Prod DB read‑only**) → Prod semantics preserved; RTM parity checks pass or are unchanged.

**5) Tests & Results (attach artifacts or links)**

* **Unit (.NET):** ☐ Added/updated ☐ Passing (attach TRX/coverage summary).
* **Integration (SP‑backed config provider, readiness):** ☐ Passing.
* **Contract (OpenAPI):** ☐ Updated ☐ Passing.
* **E2E (Gherkin):**
  + ☐ 01\_session\_establish ☐ 02\_streamed\_tool\_call ☐ 03\_background\_notification ☐ 04\_origin\_denied
* **A11y (axe):** ☐ / ☐ /sessions ☐ /config ☐ /access — **0 critical**.
* **Performance:**
  + ☐ JSON p50≤**300 ms** / p95≤**800 ms**
  + ☐ **SSE TTFB p95≤200 ms** and heartbeat cadence ≈ Network:SseKeepAliveSeconds (±1 s).

Attach artifacts: unit/integration TRX, a11y report, perf outputs, contract test logs. Evidence requirements are summarized in the Evidence Pack spec.

**6) Security & Supply Chain**

* **CodeQL** (C#/JS) clean or findings triaged with owner/date.
* **Dependency Review**: no **High/Critical** introduced.
* **Secret Scanning**: no new hits in this PR.
* **SBOM** generated/updated.

**7) Database Changes (if any)**

* **Migrations:** list files (e.g., VYYYYMMDDHHMM\_\_…sql). Confirm **add‑only**.
* **SPs:** list new/changed SPs and signatures; no breaking changes to existing contracts.
* **Grants:** confirm app role remains **EXECUTE‑only**; **no** table rights added.
* **RTM parity:** confirm RTM still points to **Prod DB read‑only** and tests use **SPs** only (no writes).

**8) Operational Readiness**

* /ready and /healthz semantics unchanged or documented; readiness gates behave as expected.
* Observability additions (metrics/logs/traces) follow conventions (no payload bodies/secrets).
* Dashboards/alerts updated if SLOs or error codes changed (Availability, JSON latency, **SSE TTFB**, heartbeat gaps, child restarts).
* **Runbooks** updated if procedures changed (deploy/rollback/incident/scale‑out/rotate license).

**9) Evidence to Attach (to Release on merge)**

* OpenAPI (spec + lint/diff), CodeQL SARIF, Dependency Review result, SBOM, unit/integration/E2E/a11y/perf artifacts, /ready & /config/effective snapshots, monitoring screenshots (post‑deploy or 24‑h). **Retention ≥ 1 year.**

**10) Screenshots / Logs (non‑secret)**

Paste or link sanitized images/logs that help reviewers (UI screenshots, dashboards, perf graphs). **No secrets**, no request bodies.

**11) Approvals & Reviewers**

* **Required CODEOWNERS** (auto‑requested): API, DB, UI, CI/CD, Security.
* **Additional reviewers:**
* **Environment approvals:** Alpha → Beta → RTM → Prod (GitHub Environments).

**12) PR Body (Markdown block to copy into GitHub)**

Paste this into the PR description field (it mirrors the checks above).

## Summary

- What & why:

- Linked issues:

## Risk & Rollback

- Impact:

- Rollback plan:

## Scope

- API/Transport: [ ] JSON [ ] SSE POST [ ] SSE GET [ ] Legacy

- UI: [ ] KendoReact [ ] Theme [ ] A11y

- DB: [ ] Migration (add-only) [ ] SP [ ] Grants

- CI/CD: [ ] Workflows [ ] CodeQL [ ] Dep Review [ ] SBOM

- Monitoring: [ ] Metrics/alerts [ ] Dashboards [ ] Synthetic

## Architecture & Compliance (REQUIRED)

- [ ] No-Hard-Coding; all dynamic values from DB SPs

- [ ] SP-only DAL; app has EXECUTE-only; no table CRUD

- [ ] Add-only DB migrations

- [ ] No secrets in code/DB/logs; secrets in GitHub Environments

- [ ] SSE pass-through (no ingress buffering); sticky by Mcp-Session-Id

- [ ] Error envelope {code,message,requestId?} for all non-2xx

- [ ] OpenAPI updated + lint/diff attached

- [ ] Alpha→Beta→RTM(Prod DB RO)→Prod semantics preserved

## Tests (attach artifacts)

- Unit: [ ] Passing

- Integration: [ ] Passing

- Contract: [ ] Passing

- E2E: [ ] 01\_session\_establish [ ] 02\_streamed\_tool\_call [ ] 03\_background\_notification [ ] 04\_origin\_denied

- A11y: [ ] 0 critical on /, /sessions, /config, /access

- Perf: [ ] JSON p50≤300ms/p95≤800ms [ ] SSE TTFB p95≤200ms; heartbeat cadence nominal

## Security & Supply Chain

- [ ] CodeQL clean/triaged

- [ ] Dependency Review (no High/Critical)

- [ ] Secret Scanning: no new findings

- [ ] SBOM updated

## Database (if any)

- Migrations: …

- SPs: …

- Grants: …

- RTM parity (Prod DB RO): …

## Operational Readiness

- Readiness/health: …

- Dashboards/alerts: …

- Runbooks: …

## Evidence (to Release on merge)

- Attach OpenAPI, lint/diff, CodeQL, Dep Review, SBOM, tests, a11y/perf, /ready, /config/effective, monitoring images (post-deploy/24h).

**13) Assumptions**

1. Reviewers enforce **merge‑queue** and required checks (build/tests, OpenAPI lint/diff, CodeQL, Dependency Review, Secret Scanning, SBOM).
2. RTM always validates on **Prod DB (read‑only)**; parity drift blocks promotion.
3. UI remains **read‑only**, CSP denies third‑party egress, and license is handled at **build time only**.

**14) Next Steps**

* Land this template into .github/pull\_request\_template.md (functional form) and keep **this .docx** as the auditable specification in /docs.
* Next recommended artifact: **.github/CODEOWNERS.docx** (and a plaintext CODEOWNERS) with path ownership for API/DB/UI/CI/CD/Docs/Security, ensuring correct approver routing in the merge queue.

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

# MCPX‑KendoBridge — Pull Request

## 1) Summary

\*\*What & why:\*\*

\*\*Linked issues:\*\* Fixes #… / Relates to #…

\*\*Change type:\*\* Feature / Fix / Refactor / Docs‑Only / CI/CD / DB‑Only (add‑only) / Security / Performance

## 2) Risk, Impact & Rollback

\*\*User impact:\*\* ☐ None ☐ Admin‑only UI ☐ API behavior (OpenAPI updated)

\*\*Operational impact:\*\* ☐ None ☐ Ingress/SSE ☐ HPA/PDB ☐ Observability

\*\*Rollback plan:\*\* link to Rollback Runbook + LKG tag

## 3) Scope (tick all)

\*\*API/Transport:\*\* ☐ `/mcp` JSON ☐ `/mcp` SSE ☐ `/mcp` GET SSE ☐ Legacy (`/messages`/`/sse`)

\*\*UI:\*\* ☐ KendoReact (read‑only) ☐ Theme (ThemeBuilder) ☐ A11y

\*\*DB:\*\* ☐ Migrations (add‑only) ☐ Stored procedures ☐ Grants/Roles

\*\*CI/CD:\*\* ☐ Workflows ☐ CodeQL ☐ Dependency Review ☐ SBOM ☐ Evidence

\*\*Monitoring:\*\* ☐ Metrics/alerts ☐ Dashboards ☐ Synthetic probes

## 4) Architecture & Compliance (REQUIRED)

- [ ] \*\*No‑Hard‑Coding.\*\* All runtime values from DB SPs (`sp\_Config\_\*`, `sp\_Feature\_IsEnabled`, `sp\_Lookup\_Get`).

- [ ] \*\*SP‑only\*\* DAL; app has \*\*EXECUTE‑only\*\*; \*\*no\*\* table CRUD.

- [ ] \*\*Add‑only\*\* DB migrations; no destructive DDL.

- [ ] \*\*Secrets\*\* not in code/DB/logs; only in \*\*GitHub Environments\*\*.

- [ ] \*\*SSE\*\* pass‑through intact (no ingress buffering); \*\*sticky\*\* by `Mcp‑Session‑Id`.

- [ ] \*\*Error envelope\*\* `{code,message,requestId?}` for all non‑2xx.

- [ ] \*\*OpenAPI\*\* (`api/openapi/mcp-proxy.yaml`) updated; \*\*lint/diff\*\* attached.

## 5) Tests & Results (attach artifacts)

- Unit (.NET): ☐ Passing (TRX)

- Integration (SP‑backed): ☐ Passing

- Contract (OpenAPI): ☐ Passing

- E2E (Gherkin): ☐ 01\_session\_establish ☐ 02\_streamed\_tool\_call ☐ 03\_background\_notification ☐ 04\_origin\_denied

- A11y (axe): ☐ 0 critical on `/`, `/sessions`, `/config`, `/access`

- Performance: ☐ JSON p50≤300 ms / p95≤800 ms; ☐ SSE TTFB p95≤200 ms

## 6) Security & Supply Chain

- [ ] \*\*CodeQL\*\* clean/triaged

- [ ] \*\*Dependency Review\*\* (no High/Critical)

- [ ] \*\*Secret Scanning\*\*: no new findings (org enforcement)

- [ ] \*\*SBOM\*\* attached

## 7) Database (if any)

\*\*Migrations:\*\* … (add‑only)

\*\*SPs:\*\* … (no breaking changes)

\*\*Grants:\*\* app role remains EXECUTE‑only

\*\*RTM parity:\*\* RTM still uses \*\*Prod DB (read‑only)\*\*

## 8) Operational Readiness

Readiness/health semantics unchanged or documented; dashboards/alerts updated; runbooks adjusted if needed.

## 9) Evidence (attach to Release)

OpenAPI lint/diff, CodeQL SARIF, Dependency Review result, SBOM, unit/integration/E2E/a11y/perf artifacts, `/ready`, `/config/effective`, monitoring screenshots (post‑deploy/24h).