**MCPX‑KendoBridge — Definition of Ready & Definition of Done (DoR / DoD)**

**Document:** docs/16\_dor\_dod.docx  
**Project Code:** MCPX‑KendoBridge  
**Version:** 1.0.0 (Draft)  
**Last Updated:** 2025‑09‑25  
**Document Owner:** DoSE (Accountable) — DocFactory (Responsible)

**Purpose.** Establish **clear, auditable entry/exit criteria** for every unit of work (Epic/Feature/Story), every change type (API, DB, UI, CI/CD, Observability), and every **environment promotion** (**Alpha → Beta → RTM → Prod**). This DoR/DoD enforces Technijian’s **GitHub‑first SDLC** (branch protections, merge queue, required checks), **No‑Hard‑Coding**, and **SP‑only** database access, and ensures all releases ship with a complete **Evidence Pack** retained **≥ 1 year**.

**DB COMPLIANCE (applies to *all* items):** **Add‑only** schema; **Stored‑procedure‑only** DAL; **No‑Hard‑Coding** of dynamic values (all config/flags/lookups must come from AppConfig/FeatureFlag via sp\_Config\_\*, sp\_Feature\_IsEnabled, sp\_Lookup\_Get); **secrets are never stored in code or DB**—use GitHub Environments/vendor portals only.

**Document Control**

**Revision History**

| **Version** | **Date** | **Author/Role** | **Summary of Changes** |
| --- | --- | --- | --- |
| 1.0.0‑D | 2025‑09‑25 | DocFactory (R) | Initial, comprehensive DoR/DoD for stories, changes, promotions, and evidence |

**Approvals**

| **Name / Role** | **Responsibility** | **Signature / Date** |
| --- | --- | --- |
| Director of Software Engineering | Accountable (A) | \_\_\_\_ / \_\_\_\_ |
| Systems Architect (T‑Arch) | Consulted (C) | \_\_\_\_ / \_\_\_\_ |
| Security Lead | Consulted (C) | \_\_\_\_ / \_\_\_\_ |
| QA Lead | Consulted (C) | \_\_\_\_ / \_\_\_\_ |
| DevOps/SRE Lead | Consulted (C) | \_\_\_\_ / \_\_\_\_ |

**Table of Contents**

1. Policy & Scope
2. DoR — Universal Checklist (applies to every Story)
3. DoR — Change‑Type Specific Checklists
4. DoD — Universal Checklist (applies to every Story)
5. DoD — Change‑Type Specific Checklists
6. Environment Promotions — Entry/Exit Criteria (Alpha → Beta → RTM → Prod)
7. Merge‑Queue & Required CI Checks (GitHub‑First)
8. Evidence Pack Requirements & Retention
9. Exceptions, Risk Acceptance & Waivers
10. Roles & Accountability (RACI excerpt)
11. Traceability to FR/NFR & Controls
12. Assumptions
13. Next Steps
14. Appendices (Ready‑to‑Paste Checklists)

**1) Policy & Scope**

* **Scope.** This DoR/DoD governs all work for MCPX‑KendoBridge: API/transport, sessioning & STDIO bridge, Origin allow‑list, health/readiness/config endpoints, observability, CI/CD, and (optional) read‑only Ops UI.
* **Policy.** No code merges to main without passing **merge queue** with required checks; no environment promotion without meeting exit criteria **and** attaching/refreshing the Evidence Pack.
* **Guardrails.** **No‑Hard‑Coding**; **SP‑only** DAL; **add‑only** migrations; **secrets only** in environment vaults; **OpenAPI 3.1** with servers for **Alpha/Beta/RTM/Prod**, bearer auth, and a standard **error envelope**; **CodeQL, Dependency Review, Secret Scanning, SBOM** required.

**2) DoR — Universal Checklist (applies to every Story)**

A Story is **Ready** only when **all** are true:

1. **Context & Scope**
   * Story references the **Epic**, links to relevant FR/NFR (by ID), and lists dependencies.
   * Problem statement and desired outcome are clear (1–3 sentences).
2. **Acceptance**
   * **Gherkin** acceptance criteria drafted and reviewed by QA (positive + at least one negative path).
   * If affecting API, **example requests/responses** (including streaming vs non‑streaming) indicated.
3. **Contract & DB**
   * **OpenAPI delta** identified (paths/headers/content negotiation/error envelope).
   * **DB impact** identified as one of: *none* / *add‑only migration* / *new SP* / *SP additive change*.
   * **SP‑only** access plan noted; **no secrets** introduced.
4. **Testing & Quality**
   * Unit/Integration/E2E coverage impact estimated; perf or a11y (if UI) tagged.
   * Required **gates** enumerated (Build/Tests, CodeQL, Dependency Review, Secret Scanning, SBOM, OpenAPI lint/diff).
5. **Security & Compliance**
   * CORS/Origin allow‑list behavior reviewed (if HTTP‑exposed).
   * Logging plan excludes sensitive payloads; error envelope usage confirmed.
6. **Operations**
   * Observability impact listed (metrics/logs/dashboards/alerts).
   * Promotion plan noted (which environments; any feature flags).

**Reminder:** All dynamic values (timeouts, keep‑alive, child command/args, allowed origins) must come from DB via sp\_Config\_\* / sp\_Feature\_IsEnabled; **no literals** in code or tests.

**3) DoR — Change‑Type Specific Checklists**

**3.1 API / Transport (includes streaming)**

* **OpenAPI 3.1** changes stubbed: servers (alpha/beta/rtm/prod), bearer, **error envelope**, **Accept: text/event-stream** negotiation.
* **Headers defined**: Mcp-Session-Id (in/out), MCP-Protocol-Version (optional), Origin.
* **SSE semantics** documented: event: message, incrementing id, heartbeat : comments at interval from Network:SseKeepAliveSeconds (DB‑sourced).
* Negative cases listed: origin denied (403), invalid session, timeouts.

**3.2 Database (schema/SPs)**

* Change is **add‑only** (no destructive DDL).
* If new SPs/params, signatures drafted with types; **EXECUTE‑only** grant plan noted.
* Migrations use naming VYYYYMMDDHHMM\_\_<slug>.sql and are **idempotent**.
* Seed values (non‑secret) documented. **No secrets in DB.**

**3.3 Observability**

* Metrics to emit/adjust listed (http\_request\_duration\_ms, stream\_first\_byte\_ms, session\_count, child\_\*).
* Log fields confirmed (requestId, sessionId, childPid) and **no payload bodies**.
* Dashboard/alert changes outlined (P1/P2 thresholds).

**3.4 UI (Optional Ops UI)**

* Design tokens in **Figma Make**; ThemeBuilder overrides planned; Kendo **Fluent v12**.
* **A11y** acceptance (axe smoke, keyboard flows) listed.
* Only **non‑secret** config shown via /config/effective.

**3.5 CI/CD & Governance**

* Workflows to touch identified; merge‑queue awareness (merge\_group) acknowledged.
* Evidence collector updates (if needed) listed.
* Environment approvals (Alpha/Beta/RTM/Prod) & secrets usage enumerated.

**4) DoD — Universal Checklist (applies to every Story)**

A Story is **Done** only when **all** are true:

1. **Build & Tests**
   * Code builds cleanly; **warnings as errors** enforced for .NET.
   * Tests pass; **coverage ≥ 80% line / ≥ 70% branch** or risk accepted by DoSE.
   * All new/changed acceptance tests (Gherkin/E2E) pass.
2. **Security & Supply Chain**
   * **CodeQL** analysis green (C# + TS if UI).
   * **Dependency Review** shows no **high** vulns introduced.
   * **Secret Scanning** clear.
   * **SBOM** generated and attached to the build artifacts.
3. **Contract & Docs**
   * **OpenAPI** updated; **lint & diff** pass; examples added for streaming where relevant.
   * Error envelope and headers reflected in contract.
   * Runbooks updated if behavior changed (deploy/rollback/incident/license rotation).
4. **DB & Config**
   * Migrations are **add‑only**, idempotent; SP signatures stable; grants applied to EXEC‑only role.
   * Seeds updated for **non‑secret** keys; **no secrets** in DB.
5. **Operations & Observability**
   * /healthz and /ready pass in target env; metrics and logs verified; no sensitive payload logging.
   * Dashboards/alerts updated if metrics changed; streaming TTFB & latency observed during smoke.
6. **Evidence**
   * Test reports, CodeQL SARIF, secret‑scan summary, SBOM, OpenAPI (with lint/diff), and any monitoring snapshots **attached to the Release** (or staging pack) with retention **≥ 1 year**.

**5) DoD — Change‑Type Specific Checklists**

**5.1 API / Transport**

* /mcp POST returns **JSON** by default; returns **SSE** when Accept: text/event-stream.
* GET /mcp supports SSE notifications (session‑scoped).
* Mcp-Session-Id echoed/issued; MCP-Protocol-Version optional.
* **Origin allow‑list** enforced from DB; 403 uses canonical error envelope.
* Streaming **TTFB ≤ 200 ms** in steady intra‑VPC conditions (perf smoke).

**5.2 Database**

* New SPs deploy cleanly; **EXECUTE‑only** grants applied; app principal lacks table SELECT.
* sp\_Config\_GetAll powers /config/effective without secrets; redaction verified.
* Migration + SP scripts included in Evidence Pack section db/.

**5.3 Observability**

* Metrics visible and sane (p50/p95 latency, session/child gauges); no high‑cardinality labels added.
* Logs contain requestId, sessionId (when present), childPid; **no payload bodies**.
* Alerts updated; silence windows documented for deployments.

**5.4 UI (Optional Ops UI)**

* Figma → ThemeBuilder tokens applied; Kendo Fluent v12 build verified.
* **Axe smoke** passes on /, /sessions, /config.
* No secrets rendered; config is read‑only and non‑secret.

**5.5 CI/CD & Governance**

* CI workflows run on pull\_request **and** merge\_group; required checks enforced.
* Deploy jobs promote Alpha → Beta → **RTM (Prod DB read‑only)** → Prod with approvals.
* Evidence collector produced/updated pack with checksums.

**6) Environment Promotions — Entry/Exit Criteria**

| **Stage** | **Entry Criteria** | **Exit (Promotion) Criteria** |
| --- | --- | --- |
| **Alpha** | Feature merged via merge‑queue; **CI gates green**; OpenAPI updated | /ready OK; basic E2E pass (UC‑01..04); initial monitoring graphs populated |
| **Beta** | Alpha exit met; perf **smoke** planned | Origin allow‑list verified; perf smoke within budgets (JSON p50≤300 ms/p95≤800 ms; TTFB≤200 ms); dashboards & alerts adjusted |
| **RTM** | Beta exit met; **Prod DB (read‑only)** credentials configured | Parity checks pass (config snapshot, /ready stability); no DB writes; Evidence Pack staged for release |
| **Prod** | RTM exit met; change window & approvals | Canary → rollout successful; 24‑hour post‑release checklist completed; Evidence Pack finalized (retained ≥ 1 year) |

**7) Merge‑Queue & Required CI Checks (GitHub‑First)**

* **Branch protections** on main; **merge queue** enabled.
* **Required checks** (block if failing): Build/Tests with coverage thresholds; **CodeQL**; **Dependency Review** (fail ≥ high severity); **Secret Scanning**; **SBOM** artifact; **OpenAPI lint & diff**.
* **CODEOWNERS** required for API/DB/security paths.

**8) Evidence Pack Requirements & Retention**

Each promotion/tagged release must attach a complete **Evidence Pack**:

* **Build/Test** results (unit/integration/E2E), coverage summary.
* **Security gates**: CodeQL SARIF, Dependency Review report, Secret‑scan summary.
* **Supply chain**: SBOM, image digest(s).
* **Contract**: OpenAPI file + lint/diff output.
* **DB**: migration log, SP signature list, /config/effective (non‑secret).
* **Ops**: /healthz & /ready smokes, **monitoring snapshot** (p50/p95, TTFB, error rate, session/child gauges).
* **Approvals**: environment approvals export, merge‑queue run summary; **retention ≥ 1 year**.

**9) Exceptions, Risk Acceptance & Waivers**

* **Exception request** must include: scope, risk analysis, compensating controls, time‑box, and rollback plan.
* **Approvals:** DoSE (A), with consultation from Security Lead and T‑Arch.
* **Examples:** temporary relaxing of a perf threshold in Beta; enabling legacy endpoints behind a flag for an interoperability trial.

**10) Roles & Accountability (RACI excerpt)**

| **Activity** | **A** | **R** | **C** | **I** |
| --- | --- | --- | --- | --- |
| Gate policy & enforcement | DoSE | SRELead | SecLead, T‑Arch | Dev, QA |
| Evidence Pack completeness | DoSE | DocFactory | QALead, SRELead, SecLead | Dev, Ops |
| DB change governance | DoSE | DBA | T‑Arch, DevLead | QA, SRE |
| OpenAPI governance | DoSE | DocFactory | DevLead, T‑Arch, SecLead | QA, Ops |
| (Full RACI in docs/14\_raci.docx.) |  |  |  |  |

**11) Traceability to FR/NFR & Controls**

* **FR‑001/002/003/…** mapped to Stories and acceptance in docs/15\_backlog.docx; DoD references OpenAPI and E2E outcomes.
* **NFR‑Performance/Availability** proven by perf smoke, monitoring snapshots, and 24‑hour post‑release checks.
* **DB COMPLIANCE** proven by migration/SP artifacts and grants in the Evidence Pack.

**12) Assumptions**

1. GitHub Environments exist for **alpha**, **beta**, **rtm**, **prod** with appropriate approvals and secrets.
2. Ingress supports **SSE** (text/event-stream) without buffering; heartbeats honored per DB config.
3. **RTM** uses **Prod DB (read‑only)** for parity validation; no writes occur from RTM.

**13) Next Steps**

1. Add the **DoR/DoD checklists** (Appendix) to the GitHub **Issue template** and **PR template**.
2. Verify merge‑queue required checks match §7 and that Evidence Pack automation matches §8.
3. Pilot a full Alpha→Prod cycle using this DoR/DoD; refine thresholds and templates as needed.

**14) Appendices (Ready‑to‑Paste Checklists)**

**A) Story DoR (paste into GitHub Issue)**

## Definition of Ready (must be true to start)

[ ] Context: Epic link + FR/NFR IDs + dependencies listed

[ ] Acceptance: Gherkin scenarios (positive + negative)

[ ] Contract: OpenAPI delta stubbed (paths/headers/content negotiation/error envelope)

[ ] DB: Impact classified; SP-only plan; add-only migration if applicable; no secrets

[ ] Testing: Unit/Integration/E2E scope + perf/a11y (if UI)

[ ] Security: Origin allow-list reviewed; error envelope usage

[ ] Operations: Metrics/logs/alerts impact; promotion & flags

**B) Story DoD (paste into GitHub PR)**

## Definition of Done (must be true to merge)

[ ] Build/Tests pass; coverage ≥ 80% line / ≥ 70% branch

[ ] Security gates green: CodeQL, Dependency Review (no high), Secret Scanning

[ ] SBOM generated and uploaded

[ ] OpenAPI updated; lint + diff clean; examples updated

[ ] DB: add-only migration applied; SP signatures stable; EXEC-only grants; no secrets in DB

[ ] Observability: /healthz & /ready ok; metrics/logs verified (no payload bodies)

[ ] Evidence: attach test reports, SARIF, secret-scan summary, SBOM, OpenAPI lint/diff; update monitoring snapshot if applicable

**C) Environment Promotion Gate**

Alpha exit → Beta entry:

[ ] /ready green; UC-01..04 pass; initial metrics OK

Beta exit → RTM entry:

[ ] Origin allow-list enforced (403 on disallowed)

[ ] Perf smoke: JSON p50≤300ms/p95≤800ms; streaming TTFB≤200ms

[ ] Dashboards/alerts adjusted

RTM exit → Prod entry (validates on Prod DB - read-only):

[ ] Parity checks: config snapshot matches expectations

[ ] Readiness stable; no DB writes from RTM

[ ] Evidence Pack prepared

Prod exit (post-release 24h):

[ ] Availability ≥ 99.9%

[ ] JSON p50≤300ms/p95≤800ms; TTFB≤200ms

[ ] Error rate < 1%; no secret leakage; snapshot exported & attached

**Footer (optional for Word header/footer):**  
*MCPX‑KendoBridge • Definition of Ready & Definition of Done • Version 1.0.0 (Draft) • 2025‑09‑25 • Confidential — Technijian Internal*