**MCPX‑KendoBridge — Security & Compliance Specification**

**Document:** docs/13\_compliance.docx  
**Project Code:** MCPX‑KendoBridge  
**Version:** 2.0.0 (Kendo Migration)  
**Last Updated:** 2025‑09‑27  
**Owner:** Security Lead (Responsible) — DoSE (Accountable) — DocFactory (Author) — SRE/QA/DBA/T‑Arch (Consulted)

**Purpose.** Define **security controls, standards mappings, and audit evidence** for MCPX‑KendoBridge across **Alpha → Beta → RTM → Prod**. This document codifies the **GitHub‑first** SDLC gates (branch protections, merge queue, CodeQL, Dependency Review, Secret Scanning, SBOM) and the project’s **data, runtime, and UI protections**, including **SSE** transport, stable **error envelope**, and admin UI **CSP**.

**DB COMPLIANCE (applies to all components):**  
**Add‑only** schema evolution; **Stored‑procedure‑only** DAL; **No‑Hard‑Coding** of dynamic values. All runtime settings (child command/args/cwd, request timeout, heartbeat cadence, Origin allow‑list, feature flags) are **DB‑sourced** via AppConfig/FeatureFlag and exposed only by **SPs** (sp\_Config\_GetValue, sp\_Config\_GetAll, sp\_Feature\_IsEnabled, sp\_Lookup\_Get). **Secrets** (e.g., SQL connection strings, Telerik license) live **only in GitHub Environments** or vendor portals—never in code, logs, or DB.

**1) Scope, Assumptions & Data Classification**

**Scope.** The **.NET 8** MCP proxy (Streamable‑HTTP + SSE), **SQL Server** (non‑secret config/flags), and optional **KendoReact admin portal (read‑only)**.

**Assumptions.**

1. **RTM** validates against **Prod DB (read‑only)**; parity drift blocks promotion.
2. Authentication is via platform **bearer**; authorization is enforced at gateway or perimeter.
3. Admin UI is **read‑only** (no writes), served from same origin as API.

**Data classification.**

| **Data Type** | **Example** | **Classification** | **Storage Location** |
| --- | --- | --- | --- |
| Non‑secret config | Security:AllowedOrigins, Network:SseKeepAliveSeconds | **Internal – Non‑secret** | SQL Server AppConfig via SPs |
| Feature flags | EnableLegacyHttpSse | **Internal – Non‑secret** | SQL Server FeatureFlag via SPs |
| Secrets (out‑of‑scope to DB) | SQL connection strings; TELERIK\_LICENSE | **Confidential – Secret** | **GitHub Environments** only |
| Telemetry (scrubbed) | requestId, sessionId, childPid | **Internal – Non‑secret** | Logs/metrics with redaction |

No PII/ePHI is processed by the service as designed; if future requirements change, trigger DPIA/PIA and update this spec.

**2) Standards & Policy Mapping**

**2.1 OWASP ASVS 4.x mapping (selected controls)**

| **ASVS Area** | **Project Control** |
| --- | --- |
| **V1 Architecture** | Threat model & DFD; trust boundaries (Internet/Ingress/API/DB/Child process); session‑per‑Mcp‑Session‑Id. See docs/17\_threat\_model.docx. |
| **V2 Auth** | Bearer token accepted at API/gateway; UI never stores or logs tokens. |
| **V3 Session** | Mcp‑Session‑Id is a routing/session key (not an auth secret); sticky routing; per‑session child isolation. |
| **V4 Access Control** | Origin allow‑list from DB; 403 origin\_forbidden envelope on mismatch. |
| **V5 Validation** | Opaque JSON‑RPC tunneled; stable error envelope; input size/timeouts via DB config. |
| **V7 Error Handling** | Canonical envelope { code, message, requestId? }; no payload bodies in logs. |
| **V9 Communications** | TLS end‑to‑end; SSE with **no ingress buffering**; heartbeats at DB cadence. |
| **V10 Malicious Inputs** | Request timeouts; stream framing; back‑pressure; structured logs for repudiation. |
| **V14 Config** | All dynamic values **DB‑sourced via SPs**; **No‑Hard‑Coding**; environment‑specific secrets in vaults. |

**2.2 Regulatory alignment (informational)**

* **HIPAA Security Rule (if handling ePHI in future):** technical safeguards—transmission security (TLS, SSE), integrity controls (structured logs, requestId), access control (gateway auth), audit controls (Evidence Pack). Currently **no ePHI** by design.
* **SOC 2 / ISO 27001** alignment (high level): change management (merge queue + approvals), secure SDLC (CodeQL/Dep Review/Secret Scanning/SBOM), incident response (runbooks), logging/monitoring (SLOs, alerts).

**3) Security Architecture Controls**

**3.1 Transport & Streaming**

* **Primary:** POST /mcp (JSON or **SSE** via Accept: text/event-stream), GET /mcp (SSE notifications).
* **Legacy (flagged):** /messages, /sse behind EnableLegacyHttpSse (default OFF). 403 feature\_disabled when off.
* **Heartbeats:** : comments at Network:SseKeepAliveSeconds (DB).
* **Ingress:** must **not buffer** text/event-stream; enforce sensible read/idle timeouts.

**3.2 Session Model**

* One **child process per Mcp‑Session‑Id** on the hosting replica; sticky routing (header hash/cookie).
* Graceful shutdown drains SSE then terminates child; readiness gates during rollout.

**3.3 Origin Policy**

* Validate Origin against **DB allow‑list** Security:AllowedOrigins; deny with stable envelope on mismatch; surface current values in /config/effective (non‑secret).

**3.4 Error Handling & Logging**

* **Envelope:** { code, message, requestId? } for all HTTP errors (e.g., origin\_forbidden, missing\_session\_id, feature\_disabled, timeout).
* **Logs:** JSON with timestamp, level, requestId, sessionId, childPid, path, status, latency\_ms, mode=json|sse; **no payload bodies**, **no secrets**.

**3.5 Admin UI (KendoReact)**

* **Theming:** Figma Make → ThemeBuilder → **Kendo Fluent v12**; import base theme then overrides.
* **CSP:** default‑deny; allow only same‑origin and known API hosts; **no external images/CDNs**; bundle local assets.
* **A11y:** WCAG 2.2 AA with axe smoke tests in CI; no token storage; no dynamic values hard‑coded.

**4) Secrets Management**

| **Secret (name)** | **Where stored** | **Accessed by** | **Notes** |
| --- | --- | --- | --- |
| SQL\_CONNECTION\_STRING (env‑scoped) | **GitHub Environments** | API | Never stored in DB/code/logs |
| SQL\_CONNECTION\_STRING\_PROD\_RO (RTM) | **GitHub Environments** | API (RTM) | Ensures **Prod DB read‑only** parity in RTM |
| TELERIK\_LICENSE / \_PATH | **GitHub Environments** | UI build (CI only) | Write to temp path during build; never ship in image |

**Rotation & exposure response:** Follow runbooks/rotate\_telerik\_license.docx and runbooks/incident.docx; sanitize logs; rotate secrets immediately if exposure suspected.

**5) Database Security & Change Management**

* **Permissions:** Create an **EXECUTE‑only** role for SPs; app principal joins the role; app has **no table rights**.
* **Migrations:** **Add‑only** scripts /db/migrations/VYYYYMMDDHHMM\_\_\*.sql; idempotent MERGE for seeds.
* **SP Contracts:** sp\_Config\_GetValue, sp\_Config\_GetAll, sp\_Feature\_IsEnabled, sp\_Lookup\_Get (@Type extensible).
* **Monitoring:** Track config\_fetch\_duration\_ms p95; investigate if >200 ms sustained.
* **Auditability:** Include applied migration list and SP signatures in the **Evidence Pack**.

**6) Supply Chain & CI/CD Safeguards (GitHub‑first)**

* **Branch protections + merge queue**; PRs require approvals per **CODEOWNERS**.
* **Required checks:** Build/Tests, **OpenAPI lint/diff**, **CodeQL** (C#/JS), **Dependency Review** (fail on **high**), **SBOM**, **Secret Scanning** (org/repo).
* **Environment promotions:** **Alpha → Beta → RTM → Prod** with approvals; **RTM** uses **Prod DB (read‑only)**; **Prod** canary + **24‑h checks**.
* **Evidence:** Retain test reports, SARIF, SBOM, OpenAPI artifacts, config/readiness snapshots, monitoring images **≥ 1 year**.

**7) Front‑End Egress, CSP & Headers**

**Content Security Policy (baseline, tighten per env):**

default-src 'none';

style-src 'self';

script-src 'self';

img-src 'self';

font-src 'self';

connect-src 'self' https://alpha.example.com https://beta.example.com https://rtm.example.com https://prod.example.com;

base-uri 'none';

frame-ancestors 'none';

**HTTP security headers (add via gateway or app):**

* X-Content-Type-Options: nosniff
* Referrer-Policy: no-referrer
* X-Frame-Options: DENY (or Content-Security-Policy: frame-ancestors 'none')
* Cross-Origin-Opener-Policy: same-origin
* Cross-Origin-Resource-Policy: same-origin
* Strict-Transport-Security: max-age=31536000; includeSubDomains (HTTPS only)

No external image/CDN usage; replace prototype avatars with local placeholders. UI consumes **/api** relative paths—**no hard‑coded hosts**.

**8) Operational Monitoring & Alerting (Security‑relevant)**

* **Policy violations:** Spike in origin\_forbidden → investigate allow‑list drift or abuse.
* **SSE quality:** **TTFB p95 ≤ 200 ms**; heartbeat gap near configured cadence; alert on drift.
* **Readiness:** restart‑to‑ready ≤ 30 s; flapping alerts escalate.
* **Logs:** ensure requestId & sessionId present; **no secrets**. Dashboards & alert policies per docs/11\_monitoring.docx.

**9) Incident Response & Vulnerability Management**

* **Incidents:** declare, triage, mitigate, communicate, verify, **post‑mortem** per runbooks/incident.docx. Include streaming issues, origin policy regressions, or secret exposures.
* **Rollback:** safe SSE drain, PDB protection; see runbooks/rollback.docx.
* **Vuln mgmt:**
  + **CodeQL:** triage weekly; fix **High/Critical** before release.
  + **Dependency Review:** block PRs introducing **High**; plan updates for Medium.
  + **SBOM:** generate each CI; attach to Release; monitor advisories.
  + **Secrets:** ensure Secret Scanning enabled; treat detections as P1 until proven benign.

**10) Compliance Evidence & Audits**

**Evidence Pack** (retain **≥ 1 year**):

* CI artifacts: tests, coverage, CodeQL SARIF, SBOM, OpenAPI lint/diff.
* Deployment approvals, RTM parity results, /config/effective snapshots (non‑secret).
* Monitoring snapshots (Availability, Latency, **SSE TTFB**, Readiness) for release + 24‑h post‑release.
* Incident and post‑mortem documents (if any).

**11) RACI (Security & Compliance)**

| **Activity** | **A** | **R** | **C** | **I** |
| --- | --- | --- | --- | --- |
| Security policy & updates | DoSE | SecLead | T‑Arch, SRE, QA, DBA | Dev |
| CI/CD gates & repo hygiene | DoSE | SRE Lead | SecLead, QA Lead | Dev |
| Secrets & license rotation | DoSE | SRE Lead | SecLead | QA |
| DB compliance & grants | DoSE | DBA | SecLead, Dev Lead | QA |
| Evidence Pack & audits | DoSE | DocFactory | QA Lead | All |

**12) Change Control & Exceptions**

* **Changes** must flow via PR + merge queue with required checks.
* **Exceptions** (e.g., emergency bypass) require **DoSE approval**, documented in the release notes, and **retro‑validation** within 24 h.

**13) Appendices**

**A) Approved Dynamic Keys & Flags (non‑secret)**

| **Key / Flag** | **Type** | **Default** | **Purpose** |
| --- | --- | --- | --- |
| Mcp:ChildCommand, Mcp:ChildArgs, Mcp:ChildCwd | string | npx, -y @progress/kendo-react-mcp@latest, `` | Child spawn (STDIO) |
| Security:AllowedOrigins | csv string | https://chat.openai.com,https://platform.openai.com | Origin allow‑list |
| Network:SseKeepAliveSeconds | int | 15 | Heartbeat cadence |
| Network:RequestTimeoutSeconds | int | 120 | E2E request timeout |
| EnableLegacyHttpSse | bool | false | Gate legacy /messages + /sse |

(Extend via **add‑only** migrations; never store secrets in DB.)

**B) Secure Config Surface**

* **GET /config/effective** returns **only non‑secret** keys shown above; redact all secret categories; add new keys to this appendix before shipping.

**C) Stable Error Codes (selection)**

* origin\_forbidden (403), missing\_session\_id (400), feature\_disabled (403), timeout (408), not\_ready (503), spawn\_failed (500). See docs/error\_catalog.docx for the full list.

**14) Next Steps**

1. Validate CSP and security headers in **Alpha**; promote through **Beta → RTM → Prod** with Evidence.
2. Ensure **Secret Scanning** is enabled and alerting to the correct team.
3. Schedule a **game day** for SSE regressions and origin policy drift.

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