**Document: 05 – Non-Functional Requirements (NFRs)**

**Project:** MCPX-KendoBridge Admin Portal  
**Document ID:** TJ-MCPX-DOC-05  
**Version:** 1.0.0  
**Status:** Draft  
**Date:** 2025-09-27  
**Owner:** Doc-Factory (Technijian)  
**Confidentiality:** Technijian Internal

**Document Control**

| **Version** | **Date** | **Author** | **Change Summary** | **Status** |
| --- | --- | --- | --- | --- |
| 0.1.0 | 2025-09-27 | Doc-Factory | Initial NFR outline aligned to Vision/FR | Draft |
| 1.0.0 | 2025-09-27 | Doc-Factory | Complete NFR set with SLOs, thresholds, verification | Draft |

**Approvals**

| **Role/Team** | **Name** | **Signature/Date** | **Comment** |
| --- | --- | --- | --- |
| Director of Software Eng. |  |  |  |
| Systems Architect |  |  |  |
| Security/Compliance |  |  |  |
| DBA |  |  |  |
| QA Lead |  |  |  |

**1. Purpose**

Define concrete **service levels, constraints, and quality attributes** for the Admin Portal and Admin API so engineering, QA, and operations can verify conformance before promotion (**Alpha → Beta → RTM → Prod**).

**2. Scope**

Applies to the **React (KendoReact Fluent 2) web app**, **.NET 8 Admin API/Workers**, **SQL Server 2022**, **Azure SSO (Entra ID)**, configuration/flags/lookups (SP-only DAL), **SSE streaming**, observability, CI/CD, security & compliance, backup/DR, and evidence retention.

**3. Service Level Objectives (SLOs)**

SLOs measured monthly unless noted. “p95/p99” are per-endpoint percentiles excluding scheduled maintenance.

| **Area / Endpoint** | **SLI Definition** | **SLO (Prod)** | **Notes / Verification** |
| --- | --- | --- | --- |
| **Availability (API)** | Minutes up / minutes in month | **≥ 99.9%** | Uptime monitor; synthetic checks |
| **Availability (Web)** | SPA served + API reachable | **≥ 99.9%** | Synthetic login → dashboard |
| **Latency JSON – read** | GET /config/effective, GET /audit (paged) | **p95 ≤ 300 ms**, **p99 ≤ 600 ms** | k6 tests; APM histograms |
| **Latency JSON – write** | Config/flags/lookups mutations | **p95 ≤ 500 ms**, **p99 ≤ 900 ms** | Contract + perf tests |
| **Health/Ready** | GET /healthz, GET /ready | **p95 ≤ 150 ms** | Smoke on each deploy |
| **SSE Time-to-First-Byte** | GET /jobs/{id}/events first event | **≤ 200 ms** | k6 + server logs |
| **SSE cadence** | Heartbeat interval | **≤ 10 s** between heartbeats | Observability alert if breached |
| **Dashboard TTI** | Initial interact time after auth | **p95 ≤ 2.0 s** | Lighthouse CI (LAN) |
| **Error rate (5xx)** | 5xx / total requests | **≤ 0.5%** | Error budget tracking |
| **Promotion readiness** | RTM ↔ Prod config parity | **0 critical diffs** | Parity gate blocks deploy |

**4. Performance & Capacity**

* **NFR-PERF-01 (Must):** The API SHALL sustain **100 RPS** (read-heavy mix 80/20) with SLOs met; tolerate **300 RPS for 5-minute bursts** with **p95 ≤ 600 ms**.  
  *Verification:* k6 load profile in CI perf stage; dashboard export attached to Evidence Pack.
* **NFR-PERF-02 (Must):** The system SHALL support **≥ 200 concurrent authenticated sessions** and **≥ 100 concurrent SSE streams** in Prod without SLO breach.  
  *Verification:* Concurrency soak test (1h), alert thresholds observed.
* **NFR-PERF-03 (Should):** Client bundle (web) SHOULD keep **JS ≤ 500 KB gz** for initial route; code-split routes for heavy pages.  
  *Verification:* Build artifact size check; Lighthouse CI budget.
* **NFR-PERF-04 (Must):** Database queries SHALL use **SPs only** and maintain **p95 ≤ 75 ms** for read paths under nominal load.  
  *Verification:* SQL Insights / Query Store percentile reports.

**5. Reliability & Resilience**

* **NFR-REL-01 (Must):** Implement **timeouts** (API→DB ≤ 30 s; API→Graph ≤ 10 s; web fetch ≤ 30 s) and **retries with jittered backoff** for idempotent calls.  
  *Verification:* Fault injection tests (network cut, latency).
* **NFR-REL-02 (Must):** SSE clients SHALL auto-reconnect with backoff; server supports **Last-Event-ID** when enabled.  
  *Verification:* Chaos tests; observe seamless resume or user notice.
* **NFR-REL-03 (Should):** Use **circuit breakers** on dependencies (DB/Graph) to protect the API during partial outages.  
  *Verification:* Chaos drill evidence.

**6. Security & Privacy**

* **NFR-SEC-01 (Must):** **Azure SSO (MSAL PKCE)** is mandatory; API validates JWT (issuer/audience/signature/exp).  
  *Verification:* AuthZ tests; pen-test report.
* **NFR-SEC-02 (Must):** **RBAC** enforced server-side (**Portal.Admin**, **Portal.Viewer**); UI hides unauthorized actions but the server is authoritative.  
  *Verification:* 403 contract tests for negative paths.
* **NFR-SEC-03 (Must):** **CORS allow-list** per environment; default-deny; changes audited (two-person rule optional).  
  *Verification:* Attempt from non-allowed origin → blocked.
* **NFR-SEC-04 (Must):** **Transport security**: TLS **1.2+**, **HSTS**, secure cookies (SameSite=Lax/Strict when applicable).  
  *Verification:* SSL Labs A rating or equivalent.
* **NFR-SEC-05 (Must):** **Secrets** never in source; stored in secret store (e.g., Key Vault/DPAPI) or environment; **/config/effective** exposes **non-secret** keys only.  
  *Verification:* Secret scanning zero critical; config contract test.
* **NFR-SEC-06 (Must):** **Data at rest** encrypted (DB TDE, disk encryption).  
  *Verification:* DBA attestation and config evidence.
* **NFR-SEC-07 (Must):** **Rate limiting** per principal/IP/session with defaults:
  + JSON: **60 req/min per principal**, **300 req/min per IP** (configurable).
  + SSE: **5 streams/principal**, **20 streams/IP** (configurable).  
    *Verification:* 429 with Retry-After when exceeded; alert on abuse.
* **NFR-SEC-08 (Should):** **Content Security Policy (CSP)** disallows unsafe-eval/inline; restricts frames to allowed origins.  
  *Verification:* Browser security scan; CSP report-only burn-in.
* **NFR-PRIV-01 (Must):** **PII minimization**; no PHI unless feature-flagged; audit access to user directory data.  
  *Verification:* Data map reviewed; privacy checklist signed.
* **NFR-SEC-09 (Must):** **Error envelope** used consistently: { code, message, details?, requestId }; never leak stack traces to clients.  
  *Verification:* Contract tests; log redaction check.

**7. Compliance & Auditability**

* **NFR-COMP-01 (Must):** Map controls to **OWASP ASVS L2** baseline and applicable **HIPAA / PCI / FFIEC** controls where scope requires.  
  *Verification:* Control matrix in Evidence Pack.
* **NFR-COMP-02 (Must):** **Audit trail** for all admin mutations (who/what/when/before→after); immutable store.  
  *Verification:* Tamper attempt fails; export contains full chain.
* **NFR-COMP-03 (Must):** **Evidence Pack** retained **≥ 1 year** per release (build/tests, CodeQL, Dependency Review, Secret Scanning, SBOM + attestation, OpenAPI lint/diff, monitoring snapshot, approvals).  
  *Verification:* Release artifact check with checksums.

**8. Observability**

* **NFR-OBS-01 (Must):** **Structured logging** with requestId/correlation IDs across web/API/worker; include role, route, outcome, latency.  
  *Verification:* Log sample inspection; trace stitching.
* **NFR-OBS-02 (Must):** **Metrics** (counters/gauges/histograms) for requests, errors, latency (p50/p95/p99), queue depth, SSE connections, heartbeat gaps, job durations.  
  *Verification:* Grafana/Insights dashboards present.
* **NFR-OBS-03 (Must):** **Alerts** for: uptime drop, error rate > 1% for 5 min, p95 latency breach, SSE heartbeat gap > 15 s, auth failures spike.  
  *Verification:* Alert policies exported to evidence.

**9. Accessibility & Usability**

* **NFR-A11Y-01 (Must):** **WCAG 2.2 AA** conformance: keyboard operability, visible focus, ARIA roles/states, contrast ≥ 4.5:1.  
  *Verification:* axe CI with zero critical; manual keyboard path.
* **NFR-A11Y-02 (Should):** Provide **skip-to-content**, focus trapping in dialogs, toast live-region announcements.  
  *Verification:* UI review + automated checks.
* **NFR-UX-01 (Should):** **Consistency via KendoReact Fluent 2** and ThemeBuilder tokens; no mixed component systems in production.  
  *Verification:* Bundle scan; code review checklist.

**10. Maintainability & Operability**

* **NFR-MAINT-01 (Must):** Code quality gates: **CodeQL** (C#/JS), **Dependency Review**, **Secret Scanning**, **lint/format**, **unit coverage ≥ 80%** on critical libraries.  
  *Verification:* CI must pass before merge.
* **NFR-MAINT-02 (Must):** **OpenAPI 3.1** is source of truth for API; breaking changes flagged and require approval.  
  *Verification:* OpenAPI diff in PR; approval record.
* **NFR-MAINT-03 (Must):** **Add-only schema**; DB changes via migration scripts named VYYYYMMDDHHmm\_\_description.sql.  
  *Verification:* Migration review; no destructive DDL in diffs.
* **NFR-OPS-01 (Must):** **Runbooks** for deploy, rollback, incident response (P1 ≤ 60-min MTTR target).  
  *Verification:* Drill once per quarter; capture notes.

**11. Portability & Compatibility**

* **NFR-PORT-01 (Must):** Browser support: latest **2** versions of Chromium-based (Edge/Chrome). Safari/Firefox best-effort. IE not supported.  
  *Verification:* CI cross-browser smoke.
* **NFR-PORT-02 (Should):** Infrastructure runs on **Windows Server 2022** VMs; containers optional; no OS-specific code in API.  
  *Verification:* Deployment doc; health checks green.

**12. Backup, Restore & DR**

* **NFR-DR-01 (Must):** **Backups**: Full nightly, differential hourly, **log every 15 min**.  
  *Verification:* Backup job evidence; restore drill logs.
* **NFR-DR-02 (Must):** **RPO ≤ 15 min**, **RTO ≤ 60 min** for API; jobs may resume or be safely re-run (idempotent).  
  *Verification:* Quarterly restore/time trial.
* **NFR-DR-03 (Should):** Offsite copy and integrity checks (checksums) for backups; alert on failures.  
  *Verification:* Backup dashboard and alerts.

**13. Internationalization & Localization**

* **NFR-I18N-01 (Won’t-for-now):** English-only UI; externalization of strings prepared for future localization.  
  *Verification:* Strings behind resource layer; lint check.

**14. Promotion Gates & Evidence**

* **NFR-GATE-01 (Must):** To promote **Alpha→Beta→RTM→Prod**, Evidence Pack contains: latest test reports, OpenAPI diff, SBOM+attestation, CodeQL & Dependency Review, secret scan, Lighthouse report, perf results, parity report, approvals.  
  *Verification:* Gate job blocks without all artifacts.

**15. Traceability (NFR ↔ FR/UC)**

| **NFR ID** | **Supports FR / UC** | **Verification Artifact** |
| --- | --- | --- |
| PERF-01/02/04 | FR-WEB/CONF/FLAGS/LOOK/JOBS; UC-02/03/07 | k6 reports; DB Query Store percentiles |
| REL-01/02/03 | UC-07 (SSE), UC-02 (Dashboard) | Chaos drills; SSE reconnect logs |
| SEC-01..09, PRIV-01 | UC-01/09/10/13 | Pen-test, 401/403 tests, CSP headers, 429 logs |
| COMP-01..03 | UC-11 | Control matrix; Evidence Pack audit |
| OBS-01..03 | UC-02/07/13 | Dashboards; alert policy export |
| A11Y-01..02 | Global | axe CI, manual review |
| MAINT-01..03 | Global | CI status; migration diffs |
| PORT-01..02 | Global | Cross-browser smoke; deploy doc |
| DR-01..03 | Global | Restore drill results |
| GATE-01 | All | Gate job logs |

**16. Assumptions & Constraints**

* Azure AD tenant and app registration exist; app roles/groups provisioned by IT.
* Non-secret config exposed via /config/effective; secrets stored in a secret store; no secrets in code.
* Network controls (Meraki/Cloudflare) enforce perimeter; CORS is **allow-list** only.
* KendoReact **Fluent 2** is the only production UI library; Figma Make + ThemeBuilder tokens are the UI SoT.

**End of Document — TJ-MCPX-DOC-05 v1.0.0**