**Document: 13 – Compliance**

**Project:** MCPX-KendoBridge Admin Portal  
**Document ID:** TJ-MCPX-DOC-13  
**Version:** 1.1.0  
**Status:** Draft  
**Date:** 2025-09-27  
**Owner:** Security & Compliance (Technijian)  
**Confidentiality:** Technijian Internal

**Document Control**

| **Version** | **Date** | **Author** | **Change Summary** | **Status** |
| --- | --- | --- | --- | --- |
| 1.0.0 | 2025-09-26 | Doc-Factory | Initial compliance baseline | Draft |
| 1.1.0 | 2025-09-27 | Security & Compliance | Align to MSAL PKCE, Kendo Fluent 2, SP-only DAL, error envelope, parity gates, Evidence Pack | Draft |

**Approvals**

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

**1. Purpose**

Define the **policies, controls, and evidence** that keep the MCPX-KendoBridge Admin Portal compliant with applicable obligations (HIPAA where PHI is in scope, PCI/FFIEC as required by clients, and **OWASP ASVS L2** security baseline). This doc ties requirements to concrete controls in architecture, code, CI/CD, and operations.

**2. Scope**

* **Systems:** Admin Web (React + KendoReact Fluent 2), Admin API (.NET 8), SQL Server 2022, Azure AD SSO (MSAL PKCE), optional Microsoft Graph, child MCP bridge (STDIO).
* **Environments:** Alpha → Beta → RTM → Prod (with RTM↔Prod config parity gate).
* **Data:** Non-secret config (exposed via /config/effective), audit events, job metadata (if persisted). Secrets are **out-of-band** (secret store), never returned by API.

**3. Data Classification & Handling**

| **Class** | **Examples** | **Handling & Storage** |
| --- | --- | --- |
| **Regulated** | PHI/PII (if tenant brings it), credentials | Not stored/returned by API; use secret store; audit all access |
| **Confidential** | Audit entries, config values (non-secret) | DB only; SP-only access; audit mutations; least privilege |
| **Internal** | Logs/metrics, parity reports, Evidence Pack | Internal repositories; redaction of identifiers where needed |
| **Public** | N/A | None |

* **Secrets policy:** No secrets in code or /config/effective.
* **Export policy:** CSV exports limited to non-secrets; role-gated.

**4. Control Framework Mapping (summary)**

| **Control Area** | **Implemented By** |
| --- | --- |
| **AuthN/SSO (ASVS 2.x, HIPAA 164.312(d))** | Azure AD (Entra ID) **MSAL PKCE**; JWT validation in API; session storage/secure cookie |
| **AuthZ/RBAC (ASVS 1.2)** | App roles/groups (**Portal.Admin**, **Portal.Viewer**); server-side enforcement; UI hides actions |
| **Transport Security (ASVS 9.x)** | TLS 1.2+, HSTS; CORS allow-list per environment |
| **Input/Output (ASVS 5/6)** | OpenAPI 3.1 validation; error **envelope** (no stack traces); content negotiation JSON/SSE |
| **Rate Limiting/Abuse (ASVS 4.3)** | Per principal/IP/session quotas; 429 with Retry-After; monitoring and alerts |
| **Secrets Mgmt (ASVS 3.6)** | Secret store; never in repo or API responses |
| **Data Access (ASVS 5.3)** | **SP-only DAL**; least-privilege EXECUTE grants; no table DML for app principal |
| **Audit & Logging (ASVS 7.x, HIPAA 164.312(b))** | Immutable **AuditEvent**; requestId; who/what/when/before→after; retention ≥ 1 year |
| **Change Mgmt (ASVS 1.5)** | CI/CD gates; OpenAPI lint/diff; CodeQL; SBOM; dependency/secret scans; Evidence Pack |
| **Availability/Resilience** | /healthz /ready; SSE **TTFB ≤ 200ms**, heartbeat ≤ 10s; rollback runbook |
| **Parity & Promotion** | RTM↔Prod **0 critical diffs** required for Prod; Evidence Pack with parity report |
| **A11y & UX (policy)** | WCAG 2.2 AA; axe CI; no security-relevant info hidden by color only |

**5. Policies (normative)**

1. **Identity & Access**
   * SSO via **MSAL PKCE**; no local passwords.
   * RBAC via AAD app roles/groups; **server authoritative**.
   * Admin consent required for Graph write; else generate Change Requests.
2. **Secure Coding**
   * **SP-only** DB access; **add-only** schema.
   * All errors use the **envelope** { code, message, details?, requestId }.
   * No secrets in repo; no secrets in /config/effective.
3. **Transport & Browser Security**
   * TLS 1.2+; HSTS.
   * **CORS allow-list** per environment; default-deny; audited edits.
   * Content Security Policy (report-only burn-in, then enforce).
4. **Observability & Audit**
   * Structured logs with requestId/role/route/status/latency.
   * **AuditEvent** for all admin mutations and sensitive reads.
   * Retain Evidence Packs and audit data ≥ 1 year.
5. **Release Governance**
   * CI gates: OpenAPI diff, CodeQL, Dependency Review, Secret Scan, SBOM, axe.
   * **Parity gate:** RTM must show **0 critical diffs** vs intended Prod config.
   * Rollback to last green release when P1.

**6. Evidence Requirements (per release)**

* **Security:** CodeQL SARIF, dependency/secret scans, CSP/HSTS presence check.
* **API:** OpenAPI lint/diff output; contract test results.
* **DB:** Migration set + hashes; **SP signature snapshot** (07a).
* **Perf:** k6 SSE TTFB/heartbeat results; latency histograms.
* **Observability:** Dashboard screenshots (Executive, SSE Health, Parity).
* **Governance:** Approvals log; **Config parity** report; runbook links.
* **Docs Visibility:** docs-md/\*\* mirror and TREE.md at release commit.

Retention: **≥ 1 year** attached to release tag.

**7. Risk Register (top items)**

| **Risk** | **Likelihood** | **Impact** | **Mitigation / Control** |
| --- | --- | --- | --- |
| CORS misconfiguration | M | H | DB-backed allow-list; two-person approval; audit; synthetics from allowed origins |
| SSE stalls / delayed first event | M | M | **TTFB ≤ 200ms** SLO; heartbeat ≤ 10s; alerts; child process restart |
| Config drift RTM↔Prod | M | H | Parity diff; **0 critical** gate; remediation tasks |
| Secret exposure via misconfigured API | L | H | No secrets in API; contract tests; scanners; code review |
| Breaking DB SP change | L | H | Signature policy; \_v2 SPs; grants PR; evidence snapshot |

**8. Third-Party & Vendor Management**

* **Azure AD / Microsoft Graph**: scope-limited; audit admin consent; review quarterly.
* **KendoReact / ThemeBuilder**: license file managed via CI secret; rotate per runbook.
* **CI/CD Actions**: pinned versions where possible; security advisories reviewed.
* **Telemetry backend**: access controlled; log redaction for PII/PHI as required.

**9. Incident Response (summary; see runbooks)**

* **P1**: Engage within 15 min; MTTR target ≤ 60 min.
* Steps: Triage → Contain (rate-limit/flag/rollback) → Eradicate → Recover → Postmortem.
* Evidence: incident timeline, requestId examples, fixed commit, updated runbooks.

**10. Training & Awareness**

* Annual secure coding training (ASVS concepts, secrets, error envelope).
* Role-based training for Admins (RBAC, audit expectations, evidence).
* Drill: parity failure & rollback once per quarter.

**11. Exceptions & Waivers**

* Document in ADR with scope, duration, compensating controls, and owner.
* Waivers expire in ≤ 90 days unless renewed; tracked in Evidence Pack.

**12. Audits & Reviews**

* Quarterly internal audit against this doc’s control list.
* Spot-check: CORS edits, AuditEvent completeness, SP signature diffs, SSE SLO adherence.
* External audits: provide Evidence Pack and signed attestations.

**13. Acceptance Criteria (Compliance)**

1. All policies in §5 enforced via code, CI, and runbooks.
2. Evidence Pack contains items in §6 for each release; retention ≥ 1 year.
3. Parity gate rejects any RTM→Prod promotion with **critical** diffs.
4. SP signature snapshot produced; any breaking change has \_v2 and ADR.
5. SSE SLOs tracked and alerted; incident procedures validated by drill.

**14. Open Issues**

* Finalize “critical vs. minor” parity keys with stakeholders.
* Confirm CSP enforcement date after report-only burn-in.
* Decide on external attestation format (e.g., in-toto/provenance for SBOM).

**End of Document — TJ-MCPX-DOC-13 v1.1.0**