# Universal Software-Driven Constraint Tracking Form

Purpose:

- This form centralizes the software-driven constraints listed in SRS section 2.4 and provides a concise, high-level mapping from each constraint to the types of backend frameworks, database classes, hosting or security controls, and verification methods that would typically be considered (presented as options or characteristics rather than a single mandated technology).

- Traceability to IEEE 29148 (SRS), ISO 26262 (safety), DO-178C (avionics), IEC 62304 (medical), and other domain-specific standards is enabled where required.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Constraint ID** | **Category** | **Constraint Description** | **Design Rationale** | **Owner** | **Impacted Requirements** | **Domain Application(s)** | **Impacted Components** | **Associated Standard(s)** | **Verification Method** | **Risk Impact** | **Status** |
| SWC-01 | Hardware | Hosting must provide enough CPU, memory and network for real-time analysis and dashboard updates | Ensure responsive UX and timely analytics under expected load | DevOps team | Perf.-related REQs | Web, Cloud, Mobile Clients | Hosting, Backend, DB, Real-time services | IEEE 29148 (Performance Constraints) | Load Test | Medium | Proposed |
| SWC-02 | Software | Backend must run on a web framework that supportsession handling and authentication. | Sessions and auth are fundamental for secure user flows and state management. | Dev Lead | Auth/session REQs | Web, Mobile-backend | Backend, Auth service, API | IEEE 29148 | Functional auth tests, security review | High | Proposed |
| SWC-03 | Software | Database must guarantee data consistency and concurrency for multiple active users | Prevent data corruption and race conditions in multi-user scenarios | DB Admin | Data integrity REQs | Web, Cloud | DB, Backend | ACID transactional DB guidance; IEEE 29148 | Concurrency tests, transactional test cases | High | Proposed |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| SWC-04 | Security / Policy | All data transmission must use secure TLS/HTTPS channels | Protect confidentiality and integrity of client-server communications | Security Team | Network/security REQs | Web, Mobile, API | Network, API, Frontend, Hosting | TLS best practices, ISO/IEC 27001 | TLS scans, pen-tests, automated HTTPS checks | High | Active |
| SWC-05 | Legal / Security | Sensitive data (passwords, secrets) must be stored only in encrypted or hashed form | Reduce risk of data breach and meet privacy obligations | Security / Dev Lead | Data storage & auth REQs | Web, Cloud | Backend, DB, Secrets mgmt | GDPR (where applicable), ISO/IEC 27001 | Code review, security audit, key-management checks | High | Proposed |
| SWC-06 | Legal | System must comply with applicable data-protection laws and institutional privacy policies | Legal compliance and user privacy are mandatory for deployment | Compliance Officer | Privacy/compliance REQs | All domains | Backend, DB, Logging, Compliance | GDPR (if applicable), local privacy laws | Compliance audit, policy review, privacy impact assessment | High | Proposed |
| SWC-07 | Policy | Access to user information must be restricted to authenticated and authorized roles | Least-privilege reduces insider/external data exposure risk | Product / Security | Access control REQs | Web, Admin tools | Backend, API, Frontend, Authz | ISO/IEC 27001, role-based access control best practices | Permission matrix tests, audit log review | High | Proposed |
| SWC-08 | Hardware / Compatibility | Deployment limited to environments compatible with standard browsers and web protocols | Ensure broad accessibility and interoperability with standard clients | Frontend Lead | Compatibility REQs | Web, Hybrid | Frontend, Hosting, API | Web standards (HTTP/HTTPS) | Cross-browser tests, protocol conformance tests | Medium | Proposed |