# **Proposed Technology Stack**

**Secure · Modular · Offline-Ready · Government Cloud Compatible**

## **1. Frontend (Web & Mobile)**

| **Layer** | **Technology** | **Rationale** |
| --- | --- | --- |
| Web UI | React.js | Open-source, widely adopted; ideal for dashboards and form-heavy apps |
| Mobile App | Flutter | Cross-platform (iOS/Android); strong offline support; performant |
| State Management | Provider / Redux | Reliable, minimal state handling across web and mobile |
| QR/RFID Scanning | Mobile APIs / Camera SDKs | Enables barcode & tag scanning without special hardware |
| UI Framework | Tailwind CSS / Flutter Widgets | Clean, accessible, responsive design |

## **2. Backend / Microservices**

| **Layer** | **Technology** | **Rationale** |
| --- | --- | --- |
| Web Framework | Node.js (NestJS) | Modular, scalable, developer-friendly architecture |
| API Gateway | Kong Gateway (OSS) | Open-source gateway with built-in security features (auth, throttling) |
| Identity & Auth | Keycloak (self-hosted) | Enterprise-grade identity provider with RBAC, MFA, and OAuth2 support |
| Messaging / Events | RabbitMQ | Lightweight broker for microservice communication and decoupling |
| Background Tasks | BullMQ (Redis-based) | Robust queue management, retries, and delayed job handling |

## **3. Data Storage & Auditability**

| **Layer** | **Technology** | **Rationale** |
| --- | --- | --- |
| Primary Database | PostgreSQL | Open-source, ACID-compliant, ideal for structured regulatory data |
| Time-Series Data | TimescaleDB (PostgreSQL) | Extension for handling sensor/grow metrics and historical insights |
| File Storage | MinIO (S3-compatible) | Self-hosted object storage for documents, images, certificates |
| Audit Trail / Logs | Elasticsearch (ELK Stack) | Centralized, visual, and searchable audit logging |

## **4. Blockchain / Immutability**

| **Objective** | **Technology** | **Rationale** |
| --- | --- | --- |
| Ledger (MVP) | Amazon QLDB | Serverless, immutable ledger for tracking state changes |
| Custom Ledger (future) | Hyperledger Fabric | For potential expansion into permissioned DLT infrastructure |
| Hash Validation | SHA-256 | Data integrity assurance for audit trails |

**5. Reporting & Analytics**

| **Component** | **Technology** | **Purpose** |
| --- | --- | --- |
| Dashboards | Metabase (self-hosted) | Open-source analytics with role-based access and visual filtering |
| Report Export | CSV / PDF via REST API | Enables compliance exports, scheduled reports, and offline access |

## **6. Mobile Offline Capability**

| **Component** | **Technology** | **Purpose** |
| --- | --- | --- |
| Local Data Storage | SQLite (Flutter) | Lightweight, persistent offline database |
| Sync Engine | Custom REST sync engine | Offline queue + sync-on-connection pattern |
| Conflict Resolution | Timestamp-based logic | Ensures no data loss during multi-user syncs |
| Secure Token Storage | flutter\_secure\_storage | Protects auth tokens and user credentials on-device |

## **7. Cloud Hosting & DevOps**

| **Layer** | **Technology / Provider** | **Rationale** |
| --- | --- | --- |
| Cloud Provider | AWS (GovCloud), Microsoft Azure, or Google Cloud | All approved for government and GDPR-regulated environments |
| Containerization | Docker / K3s | Lightweight, portable, scalable (Kubernetes-compatible) |
| Monitoring & Alerts | Prometheus + Grafana | Tracks health, resource usage, and performance |
| Logging | Loki or ELK Stack | Real-time structured logging, traceability, and audits |
| Backup / Recovery | Cron jobs + pg\_dump + MinIO/S3 snapshots | Low-cost, automatable disaster recovery |

**Note:** The system is designed for cloud-first deployment with full self-hosting capabilities. Source code, images, and documentation allow RSA or a third-party to operate the platform independently if desired.

## **8. Security Stack (CIA-Focused)**

| **Layer** | **Technology / Practice** | **Rationale** |
| --- | --- | --- |
| Authentication / Roles | Keycloak (OAuth2, RBAC, MFA) | Modular access control per user type and role |
| Encryption | TLS 1.3, AES-256, with KMS | Secures data in transit and at rest |
| Immutable Logging | Blockchain hash + audit log sync | Transparent and tamper-proof event history |
| Penetration Testing | OWASP ZAP, Nikto, Trivy | Detects runtime and dependency vulnerabilities |
| Dependency Security | Snyk, npm audit, Trivy | Prevents inclusion of vulnerable packages in build pipelines |

## **9. CI/CD & Developer Tooling**

| **Component** | **Technology** | **Purpose** |
| --- | --- | --- |
| Version Control | GitHub / GitLab / Gitea | Repository for team collaboration and secure versioning |
| CI/CD Pipeline | GitHub Actions / DroneCI | Automates build, test, and deployment workflows |
| Deployment Automation | Docker Compose / Helm | Declarative, repeatable infrastructure and service setup |
| Infrastructure as Code | Terraform / Ansible / Bash | Reproducible environment provisioning across cloud or on-premise |