BatchBuddy.AI — PLM-ERP Platform for CPG Manufacturers

# SOC 2 Readiness Control Matrix

Trust Services Criteria Mapping & Audit Retention Policy

Version 1.0 | March 2026

## Executive Summary

This document maps BatchBuddy.AI platform controls to the AICPA Trust Services Criteria (TSC) used in SOC 2 Type II examinations. This is a readiness document demonstrating that controls are implemented and prepared for future independent audit. It covers the five trust service categories: Security (CC), Availability (A), Processing Integrity (PI), Confidentiality (C), and Privacy (P). Each control is mapped to its corresponding TSC criteria with implementation status and evidence references.

## 1. Security (Common Criteria)

### 1.1 Logical Access & Authentication

| TSC Criteria | Control | Implementation | Status |
|---|---|---|---|
| CC6.1 | Role-Based Access Control | Flask-Login with admin/formulator/team roles; permission-based feature gating | ✓ Implemented |
| CC6.1 | API Key Authentication | SHA-256 hashed at rest; bb_ prefix validation; hash-only lookup (no plaintext fallback) | ✓ Implemented |
| CC6.1 | Session Management | Server-side sessions with automatic rotation; secure cookie flags; CSRF tokens on all forms | ✓ Implemented |
| CC6.2 | Multi-Factor Auth (MFA) | Enhanced admin login security; password re-auth for high-stakes AI actions | ✓ Implemented |
| CC6.3 | Least Privilege | Team permissions (view_only, can_edit, full_access); owner-scoped data isolation | ✓ Implemented |
| CC6.6 | Rate Limiting | 60 req/min per API key; configurable backend (RATELIMIT_STORAGE_URI); custom rate limiter for auth endpoints | ✓ Implemented |

### 1.2 Data Protection

| TSC Criteria | Control | Implementation | Status |
|---|---|---|---|
| CC6.7 | Encryption at Rest | PostgreSQL with TLS; Fernet encryption for sensitive fields; API keys SHA-256 hashed | ✓ **Implemented** |
| CC6.7 | Encryption in Transit | TLS 1.2+ enforced; ProxyFix for HTTPS; secure cookie flags | ✓ **Implemented** |
| CC6.1 | Credential Management | No plaintext credentials in logs; API key prefix-only display; secrets via environment variables | ✓ **Implemented** |
| CC6.8 | Input Validation | WTForms server-side validation; XSS-hardened chat widget (_esc() sanitizer); SQL injection prevention via SQLAlchemy ORM | ✓ **Implemented** |

### 1.3 Monitoring & Incident Response

| TSC Criteria | Control | Implementation | Status |
|---|---|---|---|
| CC7.1 | Audit Trail | FDA 21 CFR Part 11 compliant; before/after snapshots; IP address + user agent; immutable append-only audit_trail table | ✓ Implemented |
| CC7.2 | Security Regression Suite | 37+ automated security tests + 13 XSS tests; CI-enforced validation gates; XSS lint guard for chat widget | ✓ Implemented |
| CC7.2 | E-Signature Integrity | HMAC-SHA256 with fail-closed atomic pre-staging; all 14 AI write actions abort on e-sig failure (500 response) | ✓ Implemented |
| CC7.3 | Health Monitoring | Admin endpoint for real-time service health checks; structured logging; error tracking with monitoring system | ✓ Implemented |

### 1.4 Change Management

| TSC Criteria | Control | Implementation | Status |
|---|---|---|---|
| CC8.1 | Version Control | Git-based version control; code review process; automated checkpointing | ✓ Implemented |
| CC8.1 | Database Migrations | Alembic-managed schema migrations; idempotent startup migrations; transaction-safe with rollback on failure | ✓ Implemented |
| CC8.1 | Idempotency Controls | API write idempotency keys bound to (user_id, endpoint_path); prevents cross-endpoint replay attacks | ✓ Implemented |

## 2. Availability

| TSC Criteria | Control | Implementation | Status |
|---|---|---|---|
| A1.1 | Infrastructure | Cloud hosting with automatic scaling; PostgreSQL managed database; connection pooling with pool_pre_ping | ✓ Implemented |
| A1.2 | Backup & Recovery | PostgreSQL automated backups; soft deletion pattern for data recovery; checkpoint-based codebase recovery | ✓ Implemented |
| A1.2 | PWA Offline Support | Service worker with versioned caching for offline capabilities | ✓ Implemented |

## 3. Processing Integrity

| TSC Criteria | Control | Implementation | Status |
|---|---|---|---|
| PI1.1 | Financial Precision | All monetary values use Numeric(12,2); Decimal(str(value)) conversion pattern; database CHECK constraints | ✓ Implemented |

| TSC Criteria | Control | Implementation | Status |
|---|---|---|---|
| PI1.2 | Data Integrity Validation | Database safety system with constraint validation; FIFO inventory tracking; ALCOA data integrity principles | ✓ **Implemented** |
| PI1.3 | Atomic Operations | E-signatures atomically pre-staged before write handlers; fail-closed guarantee (no write without signature) | ✓ **Implemented** |
| PI1.4 | Webhook Audit Trail | Webhook create/delete operations logged to FDA-compliant audit trail; API-key actor resolution for non-session requests | ✓ **Implemented** |

## 4. Confidentiality

| TSC Criteria | Control | Implementation | Status |
|---|---|---|---|
| C1.1 | Data Classification | Owner-scoped data isolation; team-aware permissions; effective_owner_id pattern across all data endpoints | ✓ Implemented |
| C1.2 | Credential Protection | No API keys, tokens, or headers logged; SHA-256 hashed API keys at rest; Fernet encryption for sensitive fields | ✓ Implemented |
| C1.2 | Server-Side Data Redaction | Team members see redacted data based on permission level; server-side enforcement (not client-side) | ✓ Implemented |

## 5. Privacy

| TSC Criteria | Control | Implementation | Status |
|---|---|---|---|
| P1.1 | Privacy Policy | GDPR/CCPA compliant privacy policy; mandatory TOS acceptance at registration | ✓ Implemented |
| P6.1 | Data Retention | Soft deletion pattern preserves audit trail while honoring deletion requests; see Audit Retention Policy below | ✓ Implemented |
| P6.7 | Analytics Privacy | Privacy-friendly aggregation for button click analytics; no PII in analytics data | ✓ Implemented |

## 6. Audit Log Retention & Immutability Policy

### 6.1 Retention Requirements

All audit trail records are retained in accordance with regulatory and contractual obligations:

| Record Type | Min. Retention | Regulatory Basis | Implementation |
|---|---|---|---|
| FDA Audit Trail | 6 years | 21 CFR Part 11, Part 111 | PostgreSQL audit_trail table; append-only writes; no UPDATE/DELETE on audit rows |
| E-Signature Records | 6 years | 21 CFR Part 11 §11.50 | AiActionSignature table with HMAC-SHA256 integrity hash; bound to audit entries |
| API Access Logs | 1 year | SOC 2 CC7.1 | Structured logging with user_id, IP, user_agent; no credential data logged |
| Login Attempts | 90 days | SOC 2 CC6.1 | LoginAttempt table tracks success/failure with IP and timestamp |
| Data Change History | 6 years | FDA cGMP (21 CFR 211) | Before/after snapshots in audit_trail.record_data_before/after columns |

### 6.2 Immutability Controls

Audit log immutability is enforced through the following technical controls:

| Control | Description | Enforcement |
|---|---|---|
| Append-Only Design | Audit trail records are INSERT-only; no application code performs UPDATE or DELETE on audit rows | Application-layer enforcement; SQLAlchemy session flush pattern |
| Atomic Commit | Audit entries are added to the same database transaction as the business operation; they commit or rollback together | db.session.add() + flush() in log_compliance_action() |
| E-Signature Binding | Each e-signature includes an HMAC-SHA256 hash of the action payload, making post-hoc tampering detectable | _presage_esignature() with compute_esignature_hash() |
| Soft Deletion | User data uses soft deletion (is_deleted flag); audit trail entries are never soft-deleted | Application-layer enforcement in all delete endpoints |

### 6.3 Evidence & Examination

BatchBuddy.AI maintains the following evidence artifacts in preparation for SOC 2 Type II examination:

| Artifact | Description | Location |
|---|---|---|
| Security Regression Suite | 37+ automated tests covering CSRF, owner-scoping, credential logging, e-signature integrity, API key hashing, webhook audit, and idempotency | tests/test_security_regression.py |
| XSS Hardening Suite | 13 automated tests for chat widget XSS prevention with payload fixtures | tests/test_xss_hardening.py |
| XSS Lint Guard | Shell script enforcing innerHTML safety patterns in chat widget code | scripts/lint_xss_guard.sh |
| FDA Part 11 Whitepaper | Detailed mapping of platform features to Part 11 requirements | /trust/download/fda-part11.pdf |
| ISO 27001 Readiness | ISMS posture and Annex A control mapping with certification timeline | /trust/download/iso27001.pdf |

## Contact

Security reviews & SOC 2 evidence requests: compliance@batchbuddy.ai
Security vulnerabilities: security@batchbuddy.ai
batchbuddy.ai/trust · batchbuddy.ai/register?plan=enterprise