BatchBuddy.AI — PLM-ERP Platform for CPG Manufacturers

ISO/IEC 27001:2022 Information Security Readiness Statement

Information Security Management System — Controls Implementation Overview

Version 1.0 | March 2026

1. Purpose and Scope

This document describes BatchBuddy.AI's information security posture in relation to ISO/IEC 27001:2022, the international standard for Information Security Management Systems (ISMS). It is intended to support enterprise procurement teams, third-party risk assessors, and quality professionals evaluating BatchBuddy.AI as a software supplier.

ISO 27001 certification is a formal, audited process conducted by accredited third-party certification bodies. This document represents BatchBuddy.AI's current security controls implementation and our roadmap toward formal certification. It is not a certificate of conformance but a transparency statement demonstrating the maturity and comprehensiveness of our security program.

> ***Certification Roadmap:*** *BatchBuddy.AI is pursuing SOC 2 Type II certification as part of our long-term security roadmap. ISO 27001 formal certification is targeted for H2 2026. Enterprise customers with specific certification timelines should contact compliance@batchbuddy.ai.*

2. Information Security Controls Overview

2.1 Annex A Controls — Implementation Status

ISO 27001:2022 Annex A contains 93 controls organized into four themes: Organizational, People, Physical, and Technological. The following table summarizes BatchBuddy.AI's implementation status across the key control domains most relevant to CPG manufacturer customers.

Control Domain	Status	BatchBuddy.AI Implementation
Information Security Policies (A.5.1)	✓ **Implemented**	Formal information security policy in place; reviewed annually; available to Enterprise customers upon request under NDA.
Information Security Roles and Responsibilities (A.5.2)	✓ **Implemented**	Designated Security Officer role; clear ownership of security controls; escalation procedures defined.

Control Domain	Status	BatchBuddy.AI Implementation
Segregation of Duties (A.5.3)	✓ Implemented	Production, development, and operations environments are separated. Code deployment requires multi-person review.
Access Control Policy (A.5.15)	✓ Implemented	Role-based access control enforced at API layer. Principle of least privilege applied. Access reviewed quarterly.
Identity Management (A.5.16)	✓ Implemented	Unique user identities required. Shared accounts prohibited. Automated provisioning and de-provisioning workflows.
Authentication (A.8.5)	✓ Implemented	Strong password policy enforced (min. 12 chars, complexity). Multi-factor authentication available on Enterprise plan.
Cryptography Policy (A.5.31)	✓ Implemented	Data encrypted at rest (AES-256) and in transit (TLS 1.3 minimum). Encryption key management policy established.
Physical Security (A.7.1–7.13)	✓ Implemented	Platform hosted on AWS infrastructure with ISO 27001-certified data centers. Physical access controls managed by AWS.
Secure Development (A.8.25–8.31)	✓ Implemented	SDLC security requirements. Code review mandatory. OWASP Top 10 addressed. Dependency vulnerability scanning automated.
Vulnerability Management (A.8.8)	✓ Implemented	Automated vulnerability scanning of infrastructure and dependencies. Critical vulnerabilities patched within 72 hours.
Logging and Monitoring (A.8.15–8.16)	✓ Implemented	Centralized logging of all security events. Anomaly detection and alerting. Logs retained for minimum 12 months.
Backup (A.8.13)	✓ Implemented	Automated daily backups. Encrypted. Geographically redundant. Recovery tested quarterly.
Incident Management (A.5.24–5.28)	✓ Implemented	Formal incident response plan. Defined severity levels. Customer notification SLA for security incidents.
Supplier Relationships (A.5.19–5.22)	✓ Implemented	Third-party vendor risk assessment. Sub-processors listed in DPA. Contractual security requirements for all vendors.
Business Continuity (A.5.29–5.30)	In Progress	Business continuity plan drafted. Formal BIA in progress. RTO < 4 hours; RPO < 24 hours for production systems.
Threat Intelligence (A.5.7)	In Progress	Subscription to threat intelligence feeds. Integration with security monitoring platform in roadmap.
Secure Configuration Management (A.8.9)	✓ Implemented	Infrastructure-as-code with security baselines. Configuration drift detection. CIS benchmarks applied.
Data Leakage Prevention (A.8.12)	In Progress	DLP controls for customer formulation data in design phase. Current controls include access restrictions and audit logging.

3. Data Protection and Privacy

3.1 Customer Data Handling

BatchBuddy.AI processes customer data as a Data Processor under applicable privacy regulations. Key data protection controls include:

- Customer formulation and manufacturing data is logically isolated per account — no cross-tenant data access is possible
- Customer data is not used for any purpose other than delivering the BatchBuddy.AI service
- Customer data is not sold, shared, or disclosed to third parties except as required to deliver the service
- Data Processing Agreement (DPA) available for Enterprise customers — covers GDPR Article 28 and CCPA obligations
- Data residency: all customer data stored in US-East AWS region by default; EU region available for Enterprise customers upon request

3.2 Sub-Processors

Sub-Processor Category	Purpose	Security Certification
Cloud Infrastructure	Hosting, storage, compute, backup	AWS ISO 27001, SOC 2 Type II, FedRAMP
Email Communications	Transactional notifications, system alerts	ISO 27001 certified provider
Payment Processing	Subscription billing	PCI DSS Level 1 certified
Customer Support	Helpdesk and ticketing	SOC 2 Type II certified provider
Error Monitoring	Application performance monitoring	SOC 2 certified; no customer data transmitted

4. Security Assurance for Enterprise Customers

4.1 Available Documentation

BatchBuddy.AI provides the following security documentation to Enterprise customers under NDA upon request:

- Information Security Policy summary
- Penetration test executive summary (most recent annual test)
- Data Processing Agreement (DPA)
- Sub-processor list with security certifications
- Business Continuity and Disaster Recovery overview
- Incident Response Plan summary

4.2 Security Review Support

BatchBuddy.AI's compliance team is available to support enterprise security reviews including:

- Completion of security questionnaires (SIG Lite, CAIQ, custom)
- Calls with customer security and IT teams
- Evidence package provision for specific control inquiries
- Third-party risk assessment support

5. Continuous Improvement

Information security is not a point-in-time achievement but an ongoing program. BatchBuddy.AI operates a continuous security improvement cycle that includes:

- Annual penetration testing by accredited third-party security firms
- Quarterly internal security reviews and access audits

- Continuous automated vulnerability scanning of infrastructure and application code
- Annual security awareness training for all personnel
- Annual review and update of all information security policies
- Responsible disclosure program for security vulnerability reports

Security & Compliance Inquiries

Security reviews & documentation: compliance@batchbuddy.ai Security vulnerabilities: security@batchbuddy.ai
batchbuddy.ai/trust · batchbuddy.ai/register?plan=enterprise