Bailey’s Enterprise Software Solutions (BESS) Master Standard Operating Procedure (SOP)

Document ID	Version	Status	Classification
BESS-SOP-001	1.1	Active	Internal / Confidential
Effective Date 2026-01-12			

Positioning statement (for internal & client assurance use):
BESS engineering and security practices are *designed to align* with recognized industry standards, including ISO/IEC 12207 (software lifecycle processes) and ISO/IEC 25010 (software quality), and security frameworks including NIST CSF, CIS Controls, and OWASP Top 10. Formal certification (e.g., ISO 27001, SOC 2) may be pursued as the business scales.

1. Purpose

This SOP establishes the governance, operating rules, and minimum requirements for all BESS software work, including internal products and client deliverables, across web, mobile, desktop, APIs/microservices, and AI/ML systems.

2. Scope

- Applies to all BESS personnel (owner, employees, contractors) and to AI assistance (DeepAgent) used during delivery.
- Covers multi-tenant SaaS, single-tenant deployments, and custom client applications.
- Includes on-prem deployments (including PHI contexts) and hybrid cloud deployments.

3. Definitions

- **DeepAgent:** AI co-pilot used to accelerate delivery, governed by BESS-POL-004.
- **PII/PHI:** Personally Identifiable Information / Protected Health Information.
- **Environment:** Development, Staging, Production logical environments (may share hardware but must be isolated by configuration and deployment boundaries).

4. Governance Principles

- **Security by Design:** Security requirements are defined early, validated continuously, and verified prior to release.
- **Quality by Default:** Software must meet defined quality attributes (security, reliability, maintainability, performance, usability).
- **Ethics & Trust:** Protect client confidentiality, minimize data collection, and avoid deceptive/unsafe behavior in AI systems.

- **Traceability:** Decisions, changes, and releases must be traceable.

5. Roles & Responsibilities

5.1 Principal Engineer / Owner

- Final authority for architecture, security decisions, and production releases.
- Approves exceptions and maintains these standards.

5.2 Staff & Contractors

- Must follow all BESS SOPs/standards and complete required security/quality steps.
- Bound contractually (employment/contract terms) to comply with this SOP and related policies.

5.3 DeepAgent (AI Co-Pilot)

- May generate significant portions of design, code, and documentation.
- Cannot be the final approver for security, legal, or production release decisions.

6. Required Standards (Internal Document Set)

- **BESS-STD-002** — Software Development Lifecycle (SDLC) Standard
- **BESS-STD-003** — Security & Compliance Standard
- **BESS-POL-004** — DeepAgent Usage & Governance Policy
- **BESS-POL-005** — Code of Ethics & Professional Conduct
- **BESS-TPL-006** — Minimum Documentation Set (MDS) Template
- **BESS-STD-007** — Software Supply Chain & Licensing Standard

7. Data Handling & Privacy Baselines

- Collect and retain the minimum data needed for business and legal requirements.
- PII must be encrypted in transit (TLS) and protected at rest using strong encryption where feasible.
- PHI: default posture is on-prem client deployment unless explicitly authorized otherwise in writing.
- Access controls: least privilege; MFA required for administrative access.

8. Shared Responsibility Model (Cloud vs On-Prem)

BESS clarifies responsibilities by deployment model to reduce ambiguity and risk.

8.1 BESS-Operated (cloud/SaaS) responsibilities

- Application security, patching of application dependencies, CI/CD security, monitoring, incident response, backups (as contracted), and access management.
- Security logging and alerting appropriate to the system’s sensitivity.

8.2 Client-Operated (on-prem / client cloud) responsibilities

- Physical security, host OS patching, network firewalling, perimeter controls, and infrastructure backup unless otherwise contracted.

- BESS remains responsible for application-level security and delivering patches/updates per SLA/support terms.

9. Client Engagement & SLAs

- Every engagement must have a written scope, security expectations, and support/SLA terms.
- Security assurances must be accurate and evidence-based (no overpromising).

10. IP Protection & Reverse Engineering Mitigation

- Obfuscation is a mitigation measure, not a guarantee against reverse engineering.
- When distributing binaries, apply platform-appropriate protections and maintain release mappings/symbols per BESS-STD-002 and BESS-STD-007.
- Prefer keeping sensitive logic server-side when feasible.

11. Exceptions, Reviews, and Audits

- Any exception must be documented (ADR or formal exception record) with rationale, risk assessment, and approval.
- Annual review minimum; additional reviews after significant incidents or major architectural changes.

12. Records & Retention

- Maintain records for requirements, ADRs, threat models, test evidence, releases, and incident reports (as applicable).
- Retention periods are determined per contract and data sensitivity.

Note: This SOP defines internal policy and is not legal advice. Client-facing commitments must be made via contract/SOW and supporting evidence.