SECURITY BASECAMP

SECURE USE OF AI

Practical governance for regulated firms that want AI productivity without exposing client data, compliance obligations, or reputation.

AI can accelerate research, drafting, summarization, and workflow automation. But **secure use requires more than a policy. It requires governance, oversight, and controls** that align with current guidance from NIST, OWASP, SANS, FINRA, and the SEC.

WHY **THIS MATTERS**

AI increases speed and efficiency, but it also increases the speed of **mistakes**, **data leakage**, and **social engineering**.

Regulated firms still own supervision, customer protection, books and records, and incident response **obligations when AI is used.**

Threats now include prompt injection, sensitive information disclosure, overreliance on outputs, and **AI-enabled** fraud such as business email compromise.

WHAT SECURE AI USE LOOKS LIKE

APPROVED
TOOLS ONLY

Use vetted vendors, managed identities, and clear use-case approvals.

NO SENSITIVE DATA
BY DEFAULT

Block or restrict client data, PII, credentials, contracts, and other confidential information from **public AI tools.**

HUMAN REVIEW
BEFORE RELIANCE

Treat AI as an assistant. Humans approve client-facing, financial, supervisory, and risk-significant outputs.

LOGGING, MONITORING, AND RETENTION

Capture who used AI, for what purpose, and what records must be retained.

VENDOR AND MODEL
RISK GOVERNANCE

Assess privacy terms, training rights, prompt injection exposure, plugins, agents, and third-party dependencies.

SECURITY BASECAMP

SECURE USE OF AI

FRAMEWORK-ALIGNED **PRIORITIES**

GOVERN

Define ownership, acceptable use, approval paths, and accountability.

PROTECT

Apply Data Leakage Protection (DLP), identity controls, vendor due diligence, and secure configurations.

MONITOR

Log usage, watch for misuse, and investigate anomalies quickly.

SUPERVISE

Review high-risk outputs, customer communications, and automated actions.

RESPOND

Update incident response playbooks for AI misuse, leakage, and fraud scenarios.

HOW SECURITY BASECAMP HELPS

AI POLICY AND GOVERNANCE

Acceptable use, risk tiering, approval workflow, and regulator-ready guardrails.

CONTROL IMPLEMENTATION

DLP, Cloud Access Security Broker (CASB)/browser controls, logging, vendor reviews, and supervisory workflows.

TRAINING AND TESTING

Role-based awareness, tabletop exercises, and validation of high-risk AI use cases.

Secure AI use is not about slowing the business down. It is about enabling employees to use AI safely, defensibly, and in a way that stands up to client and regulator scrutiny.

BOOK A **RISK ASSESSMENT**

Find out where you stand in 2-3 weeks:

- Identify data exposure
- Assess SEC/FINRA alignment
- Evaluate controls
- Receive a prioritized roadmap

Based on current guidance from: NIST AI RMF 1.0 and GenAI Profile; OWASP Top 10 for LLM Applications; SANS Critical AI Security Guidelines / Secure AI Blueprint; FINRA Regulatory Notice 24-09 and 2026 GenAI trends; SEC Regulation S-P amendments.