FINRA Regulatory Alignment

Staffinity AI Platform

Aligned with FINRA Rule 4370, Regulatory Notice 24-09,

and applicable FINRA supervision requirements | Prepared May 2026

security@staffinity.io | trust.staffinity.io | staffinity.io

EXECUTIVE SUMMARY & APPLICABILITY

Staffinity, Inc. is a technology platform provider — **not a FINRA member firm**. This document describes how Staffinity's AI agent platform is architected to support FINRA member firm clients in meeting their regulatory obligations when deploying Staffinity AI agents within their organizations.

Staffinity agents are deployed as internal productivity tools via Microsoft Teams, connecting to client-controlled data sources (SharePoint, ERP, CRM). Each client deployment operates in a dedicated AWS account with per-client encryption keys, ensuring complete data isolation. This document maps Staffinity's platform capabilities to key FINRA requirements.

> **Important: Staffinity clients remain solely responsible for their own FINRA compliance. This document describes Staffinity's platform capabilities that support client compliance programs. Clients should review this document with their compliance counsel.**

Key Applicable Frameworks

Rule / Guidance	Description	Pages
FINRA Rule 4370	Business Continuity Planning — platform availability and DR obligations	3
FINRA Reg. Notice 24-09	Artificial Intelligence in the Securities Industry (2024) — explainability, bias, vendor risk	4
SEC Rule 17a-4	Books and Records — WORM electronic records retention requirements	5
FINRA Rule 3110	Supervision — oversight of AI-assisted communications via Teams	6
FINRA Rule 2010	Standards of Commercial Honor — AI fairness and bias controls	4

FINRA RULE 4370 — BUSINESS CONTINUITY PLANNING

FINRA Rule 4370 requires member firms to create and maintain a written Business Continuity Plan (BCP) that addresses how the member will address a significant business disruption. Staffinity supports member firm BCP programs by providing a highly available, resilient platform with documented recovery objectives.

Platform Availability & Redundancy

Monthly Uptime SLA	99.5% monthly uptime (Exhibit B of Master Services Agreement)
Auto-Scaling	ECS Fargate auto-scaling with minimum 1 running task maintained at all times
Multi-AZ	Multi-AZ deployment available (us-east-2 default; eu-central-1 for EU clients)
Auto Recovery	AWS Auto Recovery on infrastructure failure; ECS auto-restarts failed containers
RTO / RPO	Recovery Time Objective: <15 minutes | Recovery Point Objective: near-zero
Backup Policy	AWS Backup with 3-tier retention: daily (35 days), weekly (90 days), monthly (1 year)

Staffinity's Own BCP/DRP

Staffinity maintains its own documented business continuity and disaster recovery programs:

- Business Continuity Plan v1.0 documented (May 2026)
- Disaster Recovery Plan v1.0 documented (May 2026)
- Annual review schedule; Brent Sudeck designated as BCP/DRP Owner
- Client notification within 4 hours of P1 (Priority 1) incident
- Alternate operating procedures documented for key service functions

Vendor resilience documentation available: SLA details provided in Exhibit B of the Master Services Agreement. Staffinity BCP/DRP documentation available to qualified clients and prospects under NDA upon request. Contact: security@staffinity.io

FINRA REGULATORY NOTICE 24-09 — AI IN SECURITIES INDUSTRY

FINRA's 2024 Regulatory Notice 24-09 highlights key areas of concern for the use of AI systems in financial services, including generative AI and large language models. Staffinity's platform addresses each identified risk area:

Explainability and Transparency

- Staffinity agents use Retrieval-Augmented Generation (RAG) — answers are grounded in the client's own documents, not hallucinated from model training data.
- Source documents are cited by name in agent responses (e.g., "Per the Employee Handbook, Section 4.2...").
- System prompt and tool configuration are available for client review at any time.
- Agent behavior, capabilities, and limitations are documented in Exhibit A for each deployment.

Supervision and Control (FINRA Rule 3110)

- All agent interactions are logged in an immutable audit trail with 7-year retention (see page 5).
- Audit logs are queryable via Amazon Athena for supervisory review, e-discovery, and regulatory examination.
- Human escalation is built in — agents can be configured to route specific topics (e.g., regulatory matters) to human supervisors before responding.
- Circuit breaker triggers human review on repeated failures or anomalous behavior.

Bias and Fairness (FINRA Rule 2010)

- Agent system prompts are reviewed for neutrality and absence of discriminatory language before every deployment.
- No demographic-based differentiation in agent responses.
- Client retains full control of the system prompt — all agent instructions are auditable by the client's compliance team.
- Periodic spot-check reviews conducted by Staffinity on deployed agent behavior.

Vendor Risk Management

- Staffinity's sub-processor list is published at trust.staffinity.io/dpa.html.
- Anthropic Enterprise DPA includes explicit no-model-training clause (client data is never used to train Anthropic models).
- Annual sub-processor review; 30-day advance client notice of material sub-processor changes.
- Clients use their own Anthropic API keys — Staffinity cannot access client API credentials.

SEC RULE 17a-4 — BOOKS AND RECORDS / WORM RETENTION

SEC Rule 17a-4(f) requires broker-dealers to preserve electronic records in a "non-rewriteable, non-erasable" (WORM) format. Staffinity's audit logging architecture is specifically designed to meet this requirement:

7-Year Immutable Audit Trail Architecture

Primary Store	Amazon DynamoDB with deletion protection enabled. Every agent interaction logged with full metadata.
WORM Archive	Daily export to Amazon S3 with Object Lock in COMPLIANCE mode. 7-year retention period matches SEC Rule 17a-4 requirement.
Encryption	All audit data encrypted at rest using per-client AWS KMS Customer Managed Keys (CMK). TLS 1.3 in transit.
Querying	Amazon Athena provides SQL-based querying of S3 audit archive for supervisory review, e-discovery, and regulatory examination.
Integrity	S3 Object Lock COMPLIANCE mode prevents deletion or modification by any party — including Staffinity staff — for the retention period.

What is Logged

- Timestamp (UTC, millisecond precision)
- User identity (Microsoft Entra ID object ID)
- Session ID (unique per conversation)
- Tool calls executed (name, parameters, result)
- Response metadata (token counts, latency, model version)
- PII detection events (pattern types detected, action taken)
- Circuit breaker events (trigger conditions, escalation actions)

Note on message content logging: Full message content logging is configurable per client policy and data classification requirements. Clients operating under FINRA supervision requirements should enable full content logging to support supervisory review obligations under Rule 3110. Staffinity will assist with logging configuration during onboarding.

WORM Compliance Statement: Amazon S3 Object Lock in COMPLIANCE mode prevents the modification or deletion of any stored object for the specified retention period. No user, administrator, or AWS support staff can override this setting. This architecture satisfies the "non-rewriteable, non-erasable" requirement of SEC Rule 17a-4(f)(2)(ii)(A).

FINRA RULE 3110 — SUPERVISION OF AI-ASSISTED COMMUNICATIONS

FINRA Rule 3110 requires member firms to establish and maintain a system to supervise the activities of their associated persons. When Staffinity agents are used in client-facing, trading-adjacent, or regulated workflows within a member firm, the following platform capabilities support the firm's supervisory obligations:

Complete Communication Logging

All agent communications via Microsoft Teams are logged to the immutable audit trail (see page 5). Logs include user identity, timestamps, session context, and tool actions taken.

Reproducible Agent Behavior

Agent responses are deterministic given the same system prompt and retrieved context. Any interaction can be reproduced for supervisory review by providing the same input state.

Supervisory Query Capability

Supervisors can query audit logs via Amazon Athena by: user identity, date range, session ID, tool type, or keyword (when content logging is enabled).

Human Review Routing

Agents can be configured to flag specific topics, keywords, or query types for human review before responding. This supports pre-communication supervisory review requirements.

Change Control for Agent Instructions

System prompt changes require documented change control (Exhibit A, Section A.7). All system prompt versions are versioned and retained. Clients can review current and historical agent instructions at any time.

Client Control

Clients maintain full ownership and control over agent instructions and can modify, restrict topics, or disable the agent at any time without Staffinity involvement.

Audit Trail Access for Exams

Staffinity will provide audit log access in any format required for FINRA or SEC examination purposes. Logs can be exported as CSV, JSON, or queried via Athena.

SUMMARY CONTROLS TABLE

Rule / Requirement	Staffinity Control	Status
FINRA Rule 4370 — BCP documentation	Staffinity BCP/DRP v1.0 documented; available under NDA	Implemented
FINRA Rule 4370 — Availability SLA	99.5% monthly SLA; ECS auto-scaling; Multi-AZ option	Implemented
FINRA Rule 4370 — RTO/RPO	RTO <15 min; RPO near-zero via AWS Backup	Implemented
RN 24-09 — Explainability	RAG grounding; source citation; system prompt transparency	Implemented
RN 24-09 — Supervision & Control	7-year immutable audit trail; Athena query access	Implemented
RN 24-09 — Bias / Fairness (Rule 2010)	Neutral system prompt review; no demographic differentiation	Implemented
RN 24-09 — Vendor Risk	Sub-processor list published; Anthropic Enterprise DPA (no-training clause)	Implemented
SEC Rule 17a-4 — WORM retention	S3 Object Lock COMPLIANCE, 7-year retention; DynamoDB deletion protection	Implemented
SEC Rule 17a-4 — Accessibility	Athena SQL queries; CSV/JSON export for exam production	Implemented
FINRA Rule 3110 — Supervision	Full communication logging; supervisory query capability	Implemented
FINRA Rule 3110 — Pre-approval routing	Human review routing configurable per topic/keyword	Implemented
Encryption (FINRA IT security)	AES-256 at rest (per-client KMS CMK); TLS 1.3 in transit	Implemented
Access Control (FINRA IT security)	Microsoft Entra ID + MFA; least privilege; quarterly access reviews	Implemented
PII / Data Protection	20+ PII/PHI pattern detection; automated scanning on all messages	Implemented

COMMITMENT & CONTACT

Staffinity is committed to being a trusted technology partner for regulated financial services firms. We build our platform to make your compliance program easier, not harder. Our architecture decisions — dedicated AWS accounts per client, WORM audit trails, immutable encryption keys, full audit log accessibility — are driven by the compliance requirements our financial services clients face.

We understand that deploying AI in a regulated environment requires your compliance team, legal counsel, and technology team to have confidence in the platform. We make ourselves available for technical deep-dives, compliance reviews, and examination preparation. We want to earn your trust before you sign, and keep it every day after.

Document Information

Document Title	FINRA Regulatory Alignment — Staffinity AI Platform
Version	1.0
Prepared	May 2026
Owner	Brent Sudeck, CEO & AI Privacy and Security Officer
Intended Audience	FINRA member firm compliance officers, legal counsel, IT security teams
Classification	Staffinity Confidential — may be shared with clients and prospects under NDA

Contact for Compliance Inquiries

Security & technical questions: **security@staffinity.io**
Compliance & privacy inquiries: **privacy@staffinity.io**
Trust center and documentation: **trust.staffinity.io**